

УТВЕРЖДЕНО
Приказом председателя правления
АО «БАНК ОРЕНБУРГ»
от «23» июня 2025 года № 495
Введено в действие с
«07» июля 2025 года

**Правила подключения и эксплуатации дистанционного
банковского обслуживания в Системе
«Интернет-банк»**

(версия 1.11)

Настоящие Правила подключения и эксплуатации дистанционного банковского обслуживания в Системе «Интернет-банк» (далее по тексту - Правила):

- являются адресованным юридическим лицам, индивидуальным предпринимателям, физическим лицам, занимающимся в установленном законодательством Российской Федерации порядке частной практикой, их уполномоченным представителям, состоящим с Банком в договорных отношениях, условия которых предполагают возможность организации электронного документооборота или использования систем дистанционного банковского обслуживания (Основные договоры, кроме собственно договоров дистанционного банковского обслуживания), предложением Банка о заключении с Банком Договора дистанционного банковского обслуживания и имеют силу исключительно на территории Российской Федерации;

- устанавливают существенные условия Договора дистанционного банковского обслуживания для юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, для Участников электронного взаимодействия (далее по тексту Участники) по Договору дистанционного банковского обслуживания - Банка и Клиента.

Правила размещены в информационно-телекоммуникационной сети "Интернет" (далее по тексту – сеть «Интернет») на официальном сайте Банка <https://orbank.ru/> и действительны до момента их отмены Банком. Решение Банка об отмене Правил размещается на сайте Банка не менее чем за 10 календарных дней до даты отмены. В случае отмены Банком Правил, Заявления о присоединении к правилам подключения и эксплуатации систем дистанционного банковского обслуживания в Системе «Интернет-банк» для юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся частной практикой, поступившие после даты отмены Правил, считаются ненаправленными.

Банк вправе изменять Правила, включая приложения к ним, а также Тарифы Банка (далее по тексту - «Тарифы»). При вступлении в силу изменений в Правилах, Заявления о присоединении к правилам подключения и эксплуатации систем дистанционного банковского обслуживания в Системе «Интернет-банк» для юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся частной практикой, направленные в соответствии с ранее действовавшими Правилами и поступившие после вступления в силу изменений в Правила, считаются ненаправленными.

1. Термины и определения

Администратор Банка – уполномоченный работник Банка, обеспечивающий работоспособность Системы «Интернет-банк» и взаимодействие с Клиентом по вопросам функционирования Системы «Интернет-банк».

Администратор Клиента – уполномоченный работник Клиента, обеспечивающий формирование, учет, организацию хранения и своевременную замену ключей ЭП Клиента, а также взаимодействие с Банком по вопросам функционирования АРМ Клиента.

АРМ Клиента – автоматизированное рабочее место, установленное у Клиента, состоящее из программных средств, необходимых для работы с Сервисом.

Аккредитация – предоставление Банком возможности Клиенту обслуживаться в Системе «Интернет-банк», а также иные действия, осуществляемые Банком в соответствии с Правилами сервиса «FAKTURA.RU».

Авторизация в Сервисе (Авторизация) – процедура сравнения программными средствами Сервиса введенного Клиентом Логина с существующими в базе данных Сервиса зарегистрированными Логинами, а также проверки принадлежности Клиенту введенного Клиентом Логина (путем проверки введенного Пароля, однозначно соответствующего Логину). Клиент считается Авторизованным в Сервисе после успешного прохождения Авторизации.

Банк – Акционерное общество коммерческий банк «ОРЕНБУРГ» (АО «БАНК ОРЕНБУРГ») (Лицензия на осуществление банковских операций № 3269 от 31.03.2016, местонахождение: 460024, г. Оренбург, ул. Маршала Г.К. Жукова, зд. 25, ОГРН 1025600002230, ИНН 5612031491, КПП 561201001, БИК 045354885, к/с 30101810400000000885 в Отделении по Оренбургской области Уральского главного управления Центрального Банка Российской Федерации (Сокращенное наименование – Отделение Оренбург), официальный сайт Банка <https://orbank.ru>.

База данных – сведения, относящиеся к Клиенту и (или) его электронному средству платежа, предоставляемые Банком России и федеральным органом исполнительной власти в сфере внутренних дел о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента.

Владелец сертификата ключа проверки ЭП (Владелец ключа электронной подписи /

Владелец сертификата) - физическое лицо – уполномоченное лицо Клиента, на имя которого Удостоверяющим центром выдан Сертификат ключа проверки ЭП и которое владеет соответствующим

Ключом ЭП, позволяющим с помощью средств ЭП создавать Электронную подпись в Электронных документах (подписывать Электронные документы).

Владелец квалифицированного сертификата КЭП ФНС – юридическое лицо или индивидуальный предприниматель, которому Удостоверяющим центром ФНС РФ выдан квалифицированный сертификат ключа проверки квалифицированной электронной подписи ФНС и которое владеет соответствующим ключом КЭП ФНС, позволяющим с помощью средств криптографической защиты информации, сертифицированных ФСБ РФ, создавать квалифицированную электронную подпись в Электронных документах (подписывать Электронные документы), а также расшифровывать Электронные документы, адресованные Владелцу сертификата КЭП ФНС.

Договор дистанционного банковского обслуживания (Договор) – договор, по которому Банк предоставляет Клиенту услуги, связанные с использованием системы обмена электронными документами (Система «Интернет-банк») при осуществлении операций по счетам Клиента в рублях и иностранной валюте, открытых в Банке. Договор считается заключенным в письменной форме с момента акцепта Банком Заявления о присоединении к Правилам с подписью уполномоченного представителя Клиента, в соответствии с данными Правилами. Правила (с учетом Приложений), Заявление о присоединении к Правилам, Тарифы составляют в целом Договор.

Документ свободного формата – электронный документ (электронное сообщение, сообщение), не имеющий регламентированной структуры, подписываемый ответственным работником Банка или уполномоченным лицом Клиента посредством ЭП/КЭП ФНС/Простой ЭП, связанное с осуществлением Клиентом банковского обслуживания по открытым договорам в Банке. Вложенные в сообщения файлы могут содержать как документы в электронном виде, так и полученные с использованием сканирующих устройств изображения документов, оформленных первоначально на бумажном носителе.

Закрытый ключ ЭП (Ключ ЭП, Закрытый / Секретный ключ) – последовательность символов, которой владеет Владелец сертификата либо которая известна Владелцу сертификата ключа проверки ЭП в силу владения Сертификатом, предназначенная для создания в Электронных документах Электронной подписи с использованием Средств ЭП, а также расшифровывания ЭД, подписанных однозначно соответствующим ему Ключом проверки ЭП.

Заявление о присоединении к Правилам - составленное по форме Приложения № 3 к настоящим Правилам предложение Клиента Банку о заключении Договора без указания срока для ее акцепта.

Клиент - юридическое лицо, индивидуальный предприниматель, физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, которое, может являться владельцем ЭП/КЭП ФНС/Простой ЭП.

Клиентский менеджер – уполномоченный работник Банка, обеспечивающий взаимодействие между администратором Банка и администратором Клиента по вопросам функционирования Системы «Интернет-банк», осуществляющий аккредитацию Клиента в Системе «Интернет-банк».

Ключи ЭП (Криптографические ключи) (Ключи) – общее название Ключей электронной подписи и Ключей проверки электронной подписи, Ключей КЭП ФНС и Ключей проверки КЭП ФНС.

Квалифицированная электронная подпись ФНС (КЭП ФНС) – квалифицированная электронная подпись, квалифицированный сертификат которой выдан юридическому лицу или индивидуальному предпринимателю Удостоверяющим центром ФНС России – реквизит Электронного документа, предназначенный для защиты Электронного документа с использованием средств криптографической защиты информации (СКЗИ), сертифицированных ФСБ РФ, позволяющий идентифицировать Владейца квалифицированного сертификата КЭП ФНС, а также установить отсутствие утраты, добавления, перестановки или искажения содержащейся в Электронном документе информации после момента его подписания. КЭП ФНС может использоваться для осуществления ЭДО в рамках Системы «BeSafe» на усмотрение Организатора Сервиса, если её использование будет предусмотрено правилами Сервиса.

Ключ КЭП ФНС – уникальная последовательность символов, предназначенная для создания КЭП ФНС.

Ключ проверки КЭП ФНС – уникальная последовательность символов, однозначно связанная с ключом КЭП ФНС и предназначенная для проверки подлинности КЭП ФНС.

Квалифицированный сертификат ключа проверки КЭП ФНС (КС КЭП ФНС, Квалифицированный сертификат КЭП ФНС) – КС КЭП ФНС соответствующий требованиям, установленным Законом «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, созданный Удостоверяющим центром ФНС России.

Компрометация ключа электронной подписи (Компрометация ключа ЭП) - нарушение конфиденциальности Закрытого ключа, констатация Владейцем сертификата обстоятельств или наступление обстоятельств, при которых возможно несанкционированное использование ключа неуполномоченными лицами.

К событиям, связанным с Компрометацией ключей относятся:

- хищение, утрата или подозрение на несанкционированное копирование Ключа ЭП;

- утрата ключевых дискет или иных носителей ключа, в том числе с последующим обнаружением;
- увольнение уполномоченных лиц Клиента, имевших доступ к ключевой информации;
- хищение, утрата ключей от сейфа в момент нахождения в нем носителя ключевой информации, в том числе с последующим обнаружением;
- доступ посторонних лиц к Ключевому носителю либо подозрение, что такой доступ имел место;
- иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности несанкционированного доступа третьих лиц к Ключу ЭП.

Компрометация средств простой ЭП – нарушение конфиденциальности Средств простой электронной подписи, констатация их владельцем обстоятельств, или наступление обстоятельств, при которых возможно несанкционированное использование Средств простой электронной подписи неуполномоченными лицами.

Компрометация ключа КЭП ФНС – нарушение конфиденциальности Ключа КЭП ФНС, констатация Владелец сертификата ключа проверки КЭП ФНС обстоятельств, или наступление обстоятельств, при которых возможно несанкционированное использование Ключа КЭП ФНС неуполномоченными лицами. Действия при компрометации КЭП ФНС регламентируются нормативными и инструктивными документами ФНС.

Корпоративная информационная система «BeSafe» (КИС «BeSafe», Система) - система, организованная Закрытым акционерным обществом «Центр Цифровых Сертификатов» (630055, Новосибирская область, город Новосибирск, улица Мусы Джалиля, дом 11, ИНН 5407187087, ОГРН 1025403189602) для обеспечения договорных и технологических условий формирования и развития финансового и информационного электронного обслуживания и представляющая собой совокупность программного, информационного и аппаратного обеспечения, реализующая электронный документооборот в соответствии с «Правилами электронного документооборота корпоративной информационной системы «BeSafe» (далее по тексту – Правила BeSafe).

Логин – уникальная последовательность символов, состоящая из латинских букв и цифр, позволяющая Банку однозначно идентифицировать Клиента, в числе идентификаторов может выступать номер мобильного телефона.

Основной договор - договор банковского счета в иностранной валюте/ Условия открытия и ведения банковского счета юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся частной практикой, в АО «БАНК ОРЕНБУРГ» (в валюте РФ), Заявления о присоединении к «Условиям открытия и ведения отдельного банковского счета юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся частной практикой, в АО «БАНК ОРЕНБУРГ» (в валюте РФ)», Тарифы.

Открытый ключ ЭП (Ключ проверки ЭП, Открытый ключ) – последовательность символов, соответствующая Ключу ЭП, предназначенная для подтверждения (проверки) с использованием средств ЭП подлинности электронной цифровой подписи в электронном документе, а также зашифровывания ЭС, предназначенных владельцу Открытого ключа электронной подписи.

Оператор сервиса - ЗАО «Биллинговый центр» (ИНН 5401152049, ОГРН 1025400512400, адрес 630055, г. Новосибирск, ул. Мусы Джалиля, д. 11, офис 218), осуществляющее информационное и технологическое обслуживание Сторон в рамках Сервиса. В терминологии правил КИС «BeSafe», расположенных в Интернете по адресу www.besafe.ru, Оператор сервиса именуется Организатором Сервиса.

Подтверждение подлинности Электронной подписи в Электронном документе (проверка ЭП документа) - положительный результат, полученный в ходе проверки принадлежности Участнику Электронной подписи в Электронном документе, и отсутствие искажений в этом Электронном документе. Подтверждение подлинности Электронной подписи должно осуществляться соответствующим средством Электронной подписи с использованием Сертификата ключа проверки ЭП.

Подтверждение подлинности КЭП ФНС в Электронном документе (проверка КЭП ФНС документа) – положительный результат проверки принадлежности Электронной подписи в Электронном документе Владелец сертификата и отсутствия искажений в данном Электронном документе. Подтверждение подлинности КЭП ФНС должно осуществляться соответствующим средством Электронной подписи с использованием КС КЭП ФНС.

Простая электронная подпись (Простая ЭП) – электронная подпись, позволяющая однозначно определить авторство и составление клиентом Простого ЭД на основании сочетания предъявляемых Клиентом пары Логин и Пароль в рамках процесса Авторизации Клиента. Формирование Простого ЭД, подписанного Простой ЭП Клиента, происходит при нажатии Клиентом кнопки подписания после успешного прохождения Клиентом процесса Авторизации.

Пароль – секретная последовательность символов, которая известна только Клиенту. Пароль позволяет убедиться в том, что обратившееся лицо действительно является владельцем/уполномоченным лицом владельца представленного Логина.

Простой электронный документ (Простой ЭД) - документ, в котором информация представлена в электронно-цифровой форме, заверенный ПРОСТОЙ ЭП. Простой ЭД считается подписанным Клиентом, если он заверен ПРОСТОЙ ЭП, принадлежащей Клиенту. Клиент подтверждает Простой ЭД через ввод Разового секретного пароля при отправке Простого ЭД.

Признаки несанкционированных операций – признаки осуществления перевода денежных средств без согласия КЛИЕНТА, установленные Банком России и размещенные на его официальном сайте в информационно-телекоммуникационной сети Интернет по адресу: https://www.cbr.ru/information_security/fincert/ в соответствии с Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе».

Рисковая операция – Простой ЭД/ЭД, соответствующий одному или нескольким признакам мошеннических операций, зафиксированным во FRAMOS, за исключением Признаков несанкционированных операций.

Разовый пароль – уникальный набор символов, используемый для подтверждения Простого ЭД/ группы Простых ЭД, Авторизации Клиента и совершения иных действий. Разовый секретный пароль предоставляется Клиенту на номер мобильного телефона путем направления SMS-сообщения/PUSH-сообщения. Разовый секретный пароль имеет ограниченный срок действия, определяемый Оператором сервиса.

Разовый секретный пароль по усмотрению Оператора сервиса используется в качестве дополнительной меры защиты для подтверждения Простого ЭД / группы Простых ЭД, авторизации Клиента и совершения иных действий КЛИЕНТОМ.

Смарт-ключ – компактное программно-аппаратное устройство, предназначенное для хранения Ключа проверки ЭП, Ключа ЭП, Сертификата, а также другой электронно-цифровой информации. Смарт-ключ имеет защищенную память, где создаются и в последующем сохраняются секретные ключи ЭП. Чтение или копирование секретных ключей ЭП из защищенной памяти Смарт-ключа невозможно.

Сервис (Система «Интернет-банк») – информационно-технологический сервис, позволяющий Сторонам организовать обмен электронными документами, SMS-сообщениями, сведениями и прочей информацией, имеющей значение для Сторон (далее все вышеперечисленное именуется как - информация).

Сертификат ключа проверки электронной подписи (Сертификат, Сертификат ключа проверки ЭП, Сертификат ключа электронной подписи) – Электронный документ с Электронной подписью Удостоверяющего центра, доступный любому Участнику, включающий в себя Ключ проверки ЭП Владельца сертификата ключа проверки ЭП. Сертификаты ключей проверки ЭП выдаются Удостоверяющим центром Участнику для подтверждения подлинности ЭП и идентификации Владельца сертификата ключа проверки ЭП. Сертификат ключа проверки ЭП уникален в рамках выдавшего его Удостоверяющего центра.

Средства электронной подписи (Средства ЭП) – аппаратные и(или) программные средства, являющиеся частью средств криптографической защиты информации и реализующие хотя бы одну из следующих функций при организации Электронного документооборота: создание Электронной подписи в Электронном документе с использованием Ключа ЭП; подтверждение подлинности Электронной подписи, содержащейся в Электронном документе, с использованием Ключа проверки ЭП; создание Ключей ЭП и Ключей проверки ЭП.

Средства простой электронной подписи (Средства Простой ЭП) – материально-технические средства и информация, принадлежащие Клиенту и необходимые для создания Простой ЭП согласно технологии, определенной Сервисом.

Счет/Счета - банковский счет (счета) в рублях РФ и в иностранной валюте, открытый (е) Банком Клиенту на основании договора банковского счета в иностранной валюте/ Условий открытия и ведения банковского счета юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся частной практикой, в АО «БАНК ОРЕНБУРГ» (в валюте РФ), обслуживание которого осуществляется с использованием Системы «Интернет-банк».

Тарифы - Тарифы комиссионного вознаграждения за услуги, оказываемые юридическим лицам, индивидуальным предпринимателям и физическим лицам, занимающимся в установленном законодательством Российской Федерации порядке частной практикой (в валюте Российской Федерации) и в иностранной валюте. Тарифы размещены на информационных стендах в подразделениях Банка, в сети «Интернет» на официальном сайте Банка <https://orbank.ru>.

Усиленная неквалифицированная электронная подпись (Электронная подпись, ЭП, Электронная цифровая подпись) – реквизит Электронного документа, предназначенный для защиты Электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием Ключа электронной подписи и позволяющий идентифицировать Владельца сертификата ключа проверки электронной подписи, а также установить отсутствие утраты, добавления, перестановки или искажения содержащейся в Электронном документе информации после момента его подписания. Сертификат Электронной подписи выдан Удостоверяющим центром.

Удостоверяющий Центр – удостоверяющий центр (удостоверяющий центр «Authority»),

созданный Закрытым акционерным обществом «Центр Цифровых Сертификатов» (630055, Новосибирская область, город Новосибирск, улица Мусы Джалиля, дом 11, ИНН 5407187087, ОГРН 1025403189602), который изготавливает цифровые сертификаты для юридических и физических лиц с целью осуществления ими электронного документооборота в рамках КИС «BeSafe». Удостоверяющий центр осуществляет изготовление цифровых сертификатов в соответствии с «Правилами работы Удостоверяющего Центра (AUTHORITY)».

FRAMOS (FRAud MOnitoring System) – технологическая платформа, разработанная и принадлежащая ЗАО «ЗОЛОТАЯ КОРОНА» (ИНН 5406119655, ОГРН 1025402453438, адрес в ЕГРЮЛ: 630102, г. Новосибирск, ул. Кирова, д. 86) – далее ЗАО «ЗОЛОТАЯ КОРОНА», которая обеспечивает анализ информации, в том числе Простых ЭД/ЭД, на предмет отнесения их к Рисковым операциям и Простым ЭД/ЭД с признаками несанкционированных операций.

Электронный документооборот (ЭДО) – обмен Электронными документами и Простыми электронными документами в Системе в соответствии с настоящими Правилами.

Электронное сообщение (ЭС) – логически целостная совокупность структурированных данных, имеющих смысл для Участников информационного взаимодействия. Информация в электронном сообщении представлена в электронно-цифровой форме, позволяющей обеспечить ее обработку средствами вычислительной техники, передачу по каналам связи и хранение на машиночитаемых носителях информации.

Электронный документ (ЭД) – электронное сообщение, заверенное ЭП, в котором информация представлена в электронно-цифровой форме и соответствует установленному в рамках Системы формату. ЭД может быть преобразован в форму, пригодную для однозначного восприятия его содержания.

Термины и понятия, не указанные в настоящем разделе, используются в значениях, определенных действующим законодательством Российской Федерации, нормативными актами Банка России.

2. Общие положения

2.1. Банк предоставляет Клиенту услуги, связанные с использованием Системы «Интернет-банк» при осуществлении операций по счетам Клиента в рублях и иностранной валюте, открытых в Банке. В Системе «Интернет-банк» Банком предоставляется доступ должностным лицам Клиента к Счету(-ам), открытым для осуществления операций с денежными средствами. Права доступа к операциям по Счету(-ам) могут быть скорректированы Клиентом путем заполнения Приложения 7 к Правилам.

2.2. Стороны признают и считают бесспорной юридическую силу, полноту, точность и неизменность ЭД/Простых ЭД/ДСФ, переданных с использованием Системы «Интернет-банк», при условии положительного результата проверки ЭП/КЭП ФНС/Простой ЭП Клиента и Банка. Также Стороны признают и считают бесспорной идентичность ЭД/Простых ЭД, подписанных ЭП/КЭП ФНС/Простой ЭП, документам на бумажном носителе, подписанным уполномоченными лицами Клиента и Банка, скрепленным печатями и порождающим аналогичные права и обязанности Сторон в рамках, заключенных между ними договоров, дополнительных соглашений, соглашений и всех приложений к ним.

2.3. ЭД/Простой ЭД/ ДСФ порождает обязательства Сторон, если он надлежащим образом оформлен передающей Стороной, подписан ЭП/КЭП ФНС/Простой ЭП, зашифрован и передан по каналам связи, а принимающей Стороной расшифрован, принят и подтвержден.

2.4. Стороны признают используемые ими в соответствии с Договором средства ЭП/КЭП ФНС/Простой ЭП достаточными для подтверждения авторства и подлинности ЭД/Простых ЭД/ ДСФ, а также признают невозможность внесения изменений в ЭП/КЭП ФНС/Простой ЭП.

2.5. Стороны признают в качестве единой шкалы времени при работе в Системе «Интернет-банк» местное время по юридическому адресу Банка.

2.6. Клиент разрешает Банку, Удостоверяющему центру, Оператору сервиса и ЗАО «Золотая Корона» обработку своих персональных данных, подтверждает наличие согласия своих уполномоченных лиц на осуществление Банком, Удостоверяющим центром, Оператором сервиса и ЗАО «Золотая Корона» хранения и обработки, в том числе автоматизированной, любой информации, относящейся к персональным данным указанных лиц в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», в целях выполнения настоящих Правил, требований законодательства Российской Федерации, а также нормативных актов Банка России.

Уполномоченные лица уведомлены об обработке Банком и Удостоверяющим центром, Оператором сервиса и ЗАО «Золотая Корона» их персональных данных. Согласие субъектов персональных данных действует до момента его письменного отзыва в соответствии с требованиями действующего законодательства Российской Федерации. В случае отзыва согласия субъектом персональных данных Банк, Удостоверяющий центр, Оператор сервиса и ЗАО «Золотая Корона» имеют право продолжить обработку персональных данных на основаниях, предусмотренных действующим законодательством РФ (например, когда обработка персональных данных необходима для исполнения

требований налогового, банковского законодательства, нормативных актов Банка России).

2.7. Исполнение ЭД/Простых ЭД Клиента производится Банком не позднее рабочего дня, следующего за днем подачи Клиентом данных ЭД/Простых ЭД, при условии корректности ЭП/КЭП ФНС/Простой ЭП Клиента в ЭД/Простых ЭД, если иные сроки не установлены Основным договором, Договором, ЭД/Простым ЭД, законодательством Российской Федерации либо не вытекают из содержания ЭД/Простых ЭД.

2.8. Клиент, заключая Договор, присоединяется к Правилам электронного документооборота корпоративной информационной системы «BeSafe», размещенным в сети «Интернет» по адресу <https://besafe.ru>, к Правилам сервиса «FAKTURA.RU», размещенным в сети «Интернет» по адресу <https://bank.faktura.ru/rules>, к Правилам работы Удостоверяющего Центра «AUTHORITY», размещенными в сети «Интернет» по адресу <https://info.authority.ru>.

Правила документооборота корпоративной информационной системы «BeSafe», Правила сервиса «FAKTURA.RU», Правила работы Удостоверяющего Центра «AUTHORITY» являются неотъемлемой частью настоящих Правил и распространяются на Организатора сервиса, Участника, других Участников сервиса только в рамках их участия в работе сервиса «FAKTURA.RU».

Организатор сервиса и Участник признают, что:

- получение документа, подписанного простой электронной подписью Участника, юридически эквивалентно получению документа на бумажном носителе, заверенного собственноручной подписью Участника. Обязательства, предусмотренные настоящим пунктом, действительны при условии, что Аналог собственноручной подписи Участника создан с использованием технологии Системы «BeSafe»;

- получение документа, подписанного Электронной подписью Участника, уполномоченного лица Участника, Удостоверяющего центра юридически эквивалентно получению документа на бумажном носителе, заверенного собственноручными подписями уполномоченных лиц Участника, Удостоверяющего центра и оттиском печати Участника, Удостоверяющего центра. Обязательства, предусмотренные настоящим пунктом, действительны при условии, что Ключ электронной подписи, Электронная подпись и Сертификат ключа проверки электронной подписи Участника, уполномоченного лица Участника, Удостоверяющего центра созданы с использованием технологии Системы «BeSafe»;

- получение документа, подписанного Электронной подписью Организатора сервиса, Удостоверяющего центра юридически эквивалентно получению документа на бумажном носителе, заверенного собственноручными подписями уполномоченных лиц Организатора сервиса, Удостоверяющего центра и оттиском их печати. Обязательства, предусмотренные настоящим пунктом, действительны при условии, что Ключ электронной подписи, Электронная подпись Стороны Сертификат ключа проверки электронной подписи Организатора сервиса, Удостоверяющего центра созданы с использованием технологии Системы «BeSafe»;

- получение документа, подписанного КЭП ФНС Участника, уполномоченного лица Участника, юридически эквивалентно получению документа на бумажном носителе, заверенного собственноручными подписями уполномоченных лиц Участника, и оттиском печати Участника. Обязательства, предусмотренные настоящим пунктом, действительны при условии, что Ключ КЭП ФНС, КЭП ФНС и КС КЭП ФНС Участника, уполномоченного лица Участника созданы с использованием технологии, указанной в Регламенте УЦ ФНС.

2.9. Стороны признают, что, в целях снижения риска совершения операций без добровольного согласия Клиента или его уполномоченных лиц, Оператор сервиса с привлечением ЗАО «Золотая Корона» осуществляет обработку информации (в том числе ЭД, Простых ЭД, отправленных Клиентом, и данных Клиента) для её анализа на предмет выявления Простых ЭД, ЭД с признаками Несанкционированных операций и Рисковых операций.

2.10. Стороны осведомлены, что в соответствии со ст. 8 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платёжной системе» при выявлении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента (за исключением операции с использованием платежных карт, перевода электронных денежных средств или перевода денежных средств с использованием сервиса быстрых платежей платежной системы Банка России), Банк приостанавливает прием к исполнению распоряжения Клиента на два дня.

При выявлении Банком операции с использованием платежных карт, перевода электронных денежных средств или перевода денежных средств с использованием сервиса быстрых платежей платежной системы Банка России, соответствующих признакам осуществления перевода денежных средств без добровольного согласия Клиента, отказывает в совершении соответствующей операции (перевода).

Порядок приостановления приема к исполнению распоряжения Клиента и отказа в совершении операций (перевода) указан в п. 2.7.1, п. 2.7.2, Приложения 1 настоящих «Правил».

2.11. В целях подтверждения или опровержения факта отправки Клиентом распоряжения Стороны поручают Оператору сервиса или привлеченному ЗАО «Золотая Корона» провести проверку, позвонив по номеру телефона, предоставленному Клиентом Банку. При этом данные для идентификации Клиента или его уполномоченных лиц определяются Оператором сервиса

самостоятельно.

2.12. Стороны поручают Оператору сервиса или привлеченному ЗАО «Золотая Корона» производить запись телефонного разговора с Клиентом или его уполномоченными лицами, осуществляемого в соответствии с п. 2.11. Клиент гарантирует, что им получено согласие от его уполномоченных лиц на осуществление указанной записи телефонного разговора и её хранение. Оператор сервиса обеспечивает хранение записи телефонного разговора на защищённых носителях информации в течение 3 (Трёх) лет.

3. Заключение договора

3.1. Заключение Договора между Банком и Клиентом осуществляется путем присоединения Клиента к настоящим Правилам (акцепта Правил) в соответствии со статьей 428 Гражданского кодекса РФ и производится путем передачи Клиентом или его уполномоченным представителем в Банк Заявления о присоединении к Правилам (Приложение №3 к настоящим Правилам).

3.2. Для заключения Договора Клиент обращается к уполномоченному работнику Банка с подписанным Заявлением о присоединении к Правилам. Заявление о присоединении к Правилам подается в 2-х экземплярах. Договор считается заключенным, с момента акцепта уполномоченным работником Банка Заявления о присоединении к Правилам.

3.3. Клиент, направляя в Банк Заявление о присоединении к Правилам, принимает на себя все обязательства, установленные настоящими Правилами для Клиентов, равно как и Банк принимает на себя все обязательства, предусмотренные настоящими Правилами.

4. Порядок подключения к Системе «Интернет-банк»

4.1. Подключение и допуск к Системе «Интернет-банк» осуществляется в соответствии с Правилами сервиса «FAKTURA.RU» при условии прохождения Клиентом процедуры Аккредитации, осуществляемой Банком, а также идентификации представителей Клиента на всех этапах взаимодействия.

4.2. Подключение Клиента к Системе «Интернет-банк» производится Банком на основании Договора и в соответствии с Заявлением о присоединении к Правилам (Приложение №3 к настоящим Правилам) в течение 5 (Пяти) рабочих дней, после списания комиссии в соответствии с Тарифами.

4.3. Создание Закрытого и Открытого ключей, изготовление Сертификата ключа электронной подписи, Логина и Пароля осуществляется Банком в соответствии с требованиями Системы и законодательства Российской Федерации. Создание КЭП ФНС, КС КЭП ФНС, соответствующий требованиям, установленным Законом «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, осуществляется Удостоверяющим центром ФНС России.

4.4. При подключении Клиента к Системе «Интернет-банк», с использованием ЭП, Банк генерирует Ключи. Одна пара Ключей ЭП может быть зарегистрирована за несколькими Клиентами, уполномоченным лицом которых является одно и то же физическое лицо, на имя которого выданы соответствующие Криптографические ключи. Регистрация с использованием Криптографических ключей позволяет Клиенту создавать ЭД с использованием ЭП.

4.5. При подключении Клиента к Системе «Интернет-банк», с использованием Простой ЭП, Банк присваивает Клиенту Логин, позволяющий однозначно идентифицировать Клиента в Системе «Интернет-банк». Допускается наличие у Клиента более одного Логина. В таком случае, действие, совершенное Клиентом в Системе «Интернет-банк» под любым из Логинов, считается совершенным Клиентом. Один Логин может быть зарегистрирован за несколькими Клиентами, уполномоченным лицом которых является одно и то же физическое лицо. Для получения разовых паролей к одному Логину Клиента может быть привязан один номер мобильного телефона оператора сотовой связи, имеющий код Российской Федерации, установленный в рамках рекомендаций E.164 Международного союза электросвязи и Национальных планов нумерации телефонных номеров соответствующих стран (за исключением территорий Абхазии и Южной Осетии, где действуют коды Российской Федерации). Регистрация с использованием Простой ЭП позволяет Клиенту создавать Простые ЭД с использованием Простой ЭП.

4.6. При подключении Клиента к Системе «Интернет-банк», с использованием КЭП ФНС, Банк направляет Клиенту ссылку на регистрацию КС КЭП ФНС в Сервисе, после успешной регистрации сертификата Банк получает запрос, после обработки запроса и регистрации прав Клиент вправе осуществлять операции с использованием данного Сертификата в Сервисе. КС КЭП ФНС может быть зарегистрирован на нескольких Клиентов, уполномоченным лицом которых является одно и то же физическое лицо.

4.7. Подключение к Системе «Интернет-банк», с использованием Ключей ЭП, подтверждается Сертификатом ключа проверки электронной подписи электронного документа, формируемым Удостоверяющим центром в соответствии с требованиями Системы и законодательства Российской Федерации для подтверждения подлинности ЭП и идентификации Участника Системы. Факт выдачи

Клиенту (уполномоченному лицу Клиента) Сертификата ключа проверки электронной подписи, оформляется соответствующим Актом приема-передачи (Форма определена Правилами работы Удостоверяющего Центра «AUTHORITY») далее по тексту - акт приема-передачи), после подписания Владелец сертификата Банк регистрирует права Владельца Сертификата в Сервисе. После регистрации прав Клиент вправе осуществлять операции с использованием данного Сертификата в Сервисе.

4.8. Срок действия Сертификата ключа подписи составляет один календарный год с момента генерации Сертификата. Продление срока действия Сертификата на новый срок оформляется обязательной сменой ключей не позднее 10 (Десяти) календарных дней до момента окончания срока действия Сертификата.

4.9. Подключение к Системе «Интернет-банк» с использованием Простой ЭП подтверждается получением Клиентом Логина и Пароля. Логин отправляется на адрес электронной почты, указанной в заявлении на Выдачу Логина и Пароля (Приложение № 5 к настоящим Правилам), Пароль отправляется на номер телефона для получения разовых паролей, указанного в заявлении на Выдачу Логина и Пароля (Приложение № 5 к настоящим Правилам). После отправки Логина и Пароля Банк регистрирует права владельца Логина в Сервисе. После регистрации прав Клиент вправе осуществлять операции с использованием данного Логина в Сервисе.

4.10. Подписывая Заявление о присоединении к Правилам, Клиент подтверждает, что до заключения Договора Клиент ознакомлен и согласен с настоящими Правилами, включая информацию о любых ограничениях способов и мест использования, случаях повышенного риска использования Системы «Интернет-банк». Указанная информация размещена на сайте Банка по адресу: <https://orbank.ru/inbank/>.

5. Обязанности сторон

5.1. Стороны обязуются:

5.1.1. При исполнении Договора руководствоваться действующими законодательными актами Российской Федерации, нормативными актами Банка России, а также условиями Договора.

5.1.2. Своевременно принимать в обработку полученные ЭД/Простые ЭД/ ДСФ при успешной расшифровке полученного файла, содержащего ЭД/Простой ЭД/ ДСФ, где ЭП/КЭП ФНС/Простая ЭП электронных документов соответствуют текущим подписям зарегистрированных владельцев ЭП/КЭП ФНС/Простой ЭП.

5.1.3. Проводить плановую замену ключей ЭП (не вызванную их компрометацией) до окончания срока действия ключей ЭП.

5.1.4. В случае утери своих закрытых ключей ЭП/средств Простой ЭП, при возникновении подозрений в несанкционированном доступе к ключам и паролям или компрометации ключей иным образом, немедленно через ответственных работников Банка проинформировать противоположную Сторону и прекратить работу в Системе «Интернет-банк» на скомпрометированных ключах ЭП/КЭП ФНС/Простой ЭП до момента устранения обстоятельств, повлекших компрометацию, а также генерации, обмена и регистрации новых ключей ЭП/Пароля.

5.1.5. Не разглашать третьей стороне (за исключением случаев, предусмотренных действующим законодательством или дополнительными соглашениями Сторон) конкретные способы защиты информации, реализованные в используемой Системе «Интернет-банк».

5.1.6. Обеспечивать целостность, сохранность программных средств, архивов ЭД/Простых ЭД, протоколов работы Системы «Интернет-банк» и конфиденциальность действующей парольной и ключевой информации, используемой для разграничения доступа в Систему «Интернет-банк», шифрования данных и подтверждения авторства ЭД/Простых ЭД.

5.1.7. Организовать внутренний режим функционирования рабочего места таким образом, чтобы исключить возможность физического доступа к программно-аппаратным средствам Системы «Интернет-банк», лиц, не имеющих допуска к работе с ней, и использования паролей доступа и ключей Системы «Интернет-банк» не уполномоченными на то лицами.

5.1.8. Согласно технической документации выполнять технические требования Системы.

5.1.9. Предоставлять по требованию другой Стороне надлежащим образом оформленные ЭД/Простые ЭД/ ДСФ на бумажном носителе.

5.1.10. Обязанности Сторон в части исполнения Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» при осуществлении перевода денежных средств без добровольного согласия Клиента отражены в Условиях открытия и ведения банковского счета юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся частной практикой в АО «БАНК ОРЕНБУРГ» (в валюте РФ).

5.2. Банк обязуется:

5.2.1. Зарегистрировать Клиента в Системе «Интернет-банк», выдать владельцам ЭП Сертификаты ключей ЭП, владельцам Простой ЭП Логин и Пароль, зарегистрировать КС КЭП ФНС Клиента.

5.2.2. Ежедневно, в соответствии с установленными в разделе 2.1. Приложения № 1 к настоящим Правилам сроками, осуществлять приём от Клиента и передачу Клиенту по каналам связи надлежащим образом оформленные ЭД/Простые ЭД/ ДСФ.

5.2.3. Обеспечивать проведение консультаций Клиента по вопросам функционирования программного обеспечения АРМ Клиента.

5.2.4. Вести электронные журналы работы систем телекоммуникаций и защиты информации и архив файлов, содержащих принятые и отправленные ЭД/Простые ЭД/ ДСФ, в течение установленных действующим законодательством сроков.

5.2.5. Информировать Клиента о совершении каждой операции по банковскому счету/счетам (с использованием Системы «Интернет-банк») путем предоставления Клиенту выписки по счету/счетам в электронном виде, а также путем изменения состояния ЭД/Простого ЭД. Выписка предоставляется Клиенту автоматически по завершении каждого операционного дня, а также может быть предоставлена по его запросу.

5.2.6. Обеспечивать Клиенту возможность сообщать Банку об утрате, о получении доступа к электронному средству платежа - Системе «Интернет-банк» (оборудованию, средствам ДБО, к Сертификатам ЭП, КС КЭП ФНС, средствам Простой ЭП, средствам дополнительной защиты) лиц, не являющихся уполномоченными лицами Клиента, о совершении операций такими лицами, а также совершении операций с использованием Системы «Интернет-банк» без согласия Клиента.

5.2.7. При поступлении информации, относящейся к Клиенту и (или) его электронному средству платежа, содержащейся в Базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента, либо о совершенных противоправных действиях в отношении Клиента и (или) его электронного средства платежа, на период нахождения сведений о Клиенте и (или) его электронном средстве платежа в Базе данных, незамедлительно:

5.2.7.1 приостановить доступ к Системе «Интернет-банк» и уведомить об этом Клиента;

5.2.7.2. возобновить доступ к Системе «Интернет-банк» и уведомить об этом Клиента в случае получения в порядке, установленном Банком России, информации об исключении сведений, относящихся к Клиенту, из Базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента при отсутствии иных оснований для приостановления использования Клиентом Системе «Интернет-банк» в соответствии с законодательством Российской Федерации.

5.2.8. Предоставить Клиенту информацию о приостановлении или прекращении использования им Системы «Интернет-банк» в день такого приостановления или прекращения с указанием причины. Уведомление направляется Клиенту на адрес электронной почты либо номер мобильного телефона, указанный в Заявлении о присоединении к Правилам.

5.3. Клиент обязуется:

5.3.1. Самостоятельно и за свой счет обеспечить наличие аппаратных и программных средств, необходимых для функционирования клиентской части системы, подключение своих вычислительных средств к сети «Интернет», доступ к сети «Интернет», а также защиту собственных вычислительных средств и криптографических ключей, мобильных устройств и паролей от несанкционированного доступа, и вредоносного программного обеспечения.

5.3.2. Выполнять рекомендации по обеспечению безопасности и защите информации (Приложение № 2 к настоящим Правилам).

5.3.3. Оплачивать комиссионное вознаграждение Банку в соответствии с Тарифами.

5.3.4. Проводить электронные расчёты АРМ Клиента только на исправном и проверенном на отсутствие вирусов оборудовании.

5.3.5. Назначить уполномоченного работника, отвечающего за формирование, учет, смену и организацию хранения ключей Клиента, используемых в Системе «Интернет-банк», с учетом обеспечения их конфиденциальности, а также за защиту АРМ Клиента от несанкционированного доступа и поддержание средств защиты информации в рабочем состоянии.

5.3.6. Организовать внутренний режим функционирования АРМ Клиента таким образом, чтобы исключить возможность использования Системы «Интернет-банк» лицами, не имеющими на то полномочий, при подключении с использованием Простой ЭП, при первом входе заменить временный Пароль, используемый для Авторизации в Системе «Интернет-банк».

5.3.7. Самостоятельно контролировать срок действия Сертификатов ключей ЭП и своевременно (не менее чем за 10 (Десять) календарных дней до окончания срока их действия) инициировать процедуру смены Сертификатов ключей ЭП. Для КС КЭП ФНС сроки и процедура смены устанавливается регламентом УЦ ФНС.

5.3.8. Обеспечивать передачу по каналам связи в адрес Банка надлежащим образом оформленные ЭД/Простые ЭД.

5.3.9. Ежедневно осуществлять вход в Систему «Интернет-банк» для получения информации от Банка о состоянии ЭД/Простых ЭД/ ДСФ, о состоянии счета/счетов в целях проверки проведенных

Банком операций, а также для получения иных сообщений. Обязанность Банка по информированию Клиента о совершении операции с использованием Сервиса считается исполненной с момента, когда сведения об операции, совершенной в Сервисе, становятся доступны Клиенту.

5.3.10. Немедленно прекратить отправку ЭД/Простых ЭД/ ДСФ и незамедлительно сообщить в Банк, направить уведомление в письменной форме в Банк о компрометации ключей ЭП, ключей КЭП ФНС, средств ЭП/Простой ЭП для необходимости блокирования доступа к Системе «Интернет-банк» в связи с возникновением угрозы доступа или доступом к Системе «Интернет-банк», ключевой информации, ЭП и Сертификатам, Средствам ЭП/Простой ЭП неуполномоченных лиц, а также при наступлении следующих обстоятельств:

- при обнаружении операций, которых Клиент не совершал;
- при утере носителя уникальной ключевой информации или подозрении насчёт его использования и/или копирования третьими лицами;
- при прекращении (истечении срока) полномочий уполномоченного лица Клиента, которому принадлежит ЭП/КЭП ФНС/Простая ЭП;
- при утрате ключа ЭП, ключа КЭП ФНС, средств Простой ЭП, совершении операций с его использованием без согласия Клиента (его уполномоченных лиц). Уведомление может быть передано по телефону, факсу, электронной почте или иным способом при условии, что на основании представленной Клиентом в Банк информации у Банка не возникает сомнений, что такое уведомление исходит от Клиента.

5.3.11. Выполнять иные обязанности, предусмотренные приложениями к Правилам.

5.3.12. За собственный счёт поддерживать в рабочем состоянии программно-технические средства, обеспечивающие функционирование Системы «Интернет-банк», и восстанавливать работоспособность АРМ Клиента или мобильного устройства, нарушенную по его вине.

5.3.13. Своевременно проводить обновление программного обеспечения, используемого для работы АРМ или мобильного устройства Клиента, при получении соответствующего уведомления от Банка или от Сервиса Faktura.ru.

5.3.14. При смене лиц, являющихся владельцами ключей ЭП, КЭП ФНС, Простой ЭП, а также внесении изменений в карточку с образцами подписей и оттиска печати, смене местонахождения, правового статуса, телефонов, внесении изменений и дополнений в учредительные документы письменно сообщать Банку об этом в течение 3 (Трех) рабочих дней, с обязательным предоставлением документов, подтверждающих изменение сведений.

До поступления сообщения об указанных изменениях и до внесения соответствующих изменений и дополнений в Договор все действия, совершенные по ранее указанным Клиентом реквизитам, считаются совершенными законно и засчитываются как выполнение Сторонами своих обязательств.

5.3.15. В случае прекращения действия Договора вернуть предоставленные Банком смарт-ключи и пароли.

5.3.16. Обеспечить:

- предоставление физическими лицами, уполномоченными Клиентом распоряжаться денежными средствами на Счете и/или получать от Банка информацию о состоянии Счета или иную информацию в связи с наличием Счета, своих персональных данных Банку;

- предоставление вышеуказанными и иными физическими лицами, чьи персональные данные содержатся в представляемых Клиентом Банку, Удостоверяющему центру, Оператору сервиса и ЗАО «Золотая корона» документах, согласия на обработку персональных данных, включая автоматизированную обработку этих данных Банком, Удостоверяющим центром, Оператором сервиса и ЗАО «Золотая корона», в соответствии с требованиями действующего законодательства Российской Федерации.

6. Права сторон

6.1. Стороны имеют право:

6.1.1. Передавать другой Стороне или получать от другой Стороны электронные документы в соответствии со списком, приведенным в разделе 1 Приложения № 1 к настоящим Правилам.

6.1.2. Запрашивать надлежащим образом оформленные бумажные копии электронных документов.

6.1.3. Права Сторон в части исполнения Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» при осуществлении перевода денежных средств без добровольного согласия Клиента отражены в Условиях открытия и ведения банковского счета юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся частной практикой в АО «БАНК ОРЕНБУРГ» (в валюте РФ).

6.2. Банк имеет право:

6.2.1. Списывать со Счета на условиях заранее данного акцепта Клиента суммы комиссионных

вознаграждений (в соответствии с Тарифами) по мере предоставления Банком услуг по Договору.

6.2.2. Производить замену программного обеспечения Системы «Интернет-банк», изменять требования к аппаратно-программным средствам Клиента, форматы и список ЭД/Простых ЭД, а также изменять порядок работы в Системе «Интернет-банк».

6.2.3. Изменять Тарифы с предварительным уведомлением Клиента, не позднее чем за 10 (Десять) календарных дней до вступления указанных изменений в силу, путем размещения соответствующей информации на информационных стендах в подразделении Банка, в сети «Интернет» на официальном сайте Банка (<https://orbank.ru>).

6.2.4. Приостанавливать прием и отправку ЭД/Простых ЭД с использованием Системы «Интернет-банк» в случае неисполнения Клиентом обязательств по уплате Банку комиссионного вознаграждения в соответствии с Тарифами.

При этом Клиент не освобождается от обязанности уплачивать Банку комиссионное вознаграждение в соответствии с Тарифами.

6.2.5. По просьбе Клиента возобновить прием и отправку ЭД/Простых ЭД с использованием Системы «Интернет-банк» не позднее дня, следующего после дня уплаты Клиентом Банку комиссионного вознаграждения, в соответствии с Тарифами.

6.2.6. В случае замены карточки с образцами подписей клиента и оттиска печати и/или поступления в Банк надлежащим образом оформленных документов о смене уполномоченных лиц Клиента приостанавливать прием и отправку электронных документов Клиента с использованием Системы «Интернет-банк» (до момента регистрации новых Владельцев сертификатов ключей ЭП, КС КЭП ФНС и Простой ЭП), а также в иных случаях, предусмотренных действующим законодательством Российской Федерации, нормативными актами Банка России, настоящими Правилами.

6.2.7. После предварительного предупреждения отказывать Клиенту в приеме от него распоряжений на проведение операции по банковскому счету (вкладу), подписанных ЭП/КЭП ФНС/Простой ЭП, в случае выявления подозрительных операций Клиента, при этом Банк принимает от таких Клиентов только надлежащим образом оформленные расчетные документы на бумажном носителе.

6.2.8. Банк оставляет за собой право отказывать Клиенту в приеме от него распоряжения на проведение операции по Счету, подписанному ЭП/КЭП ФНС/Простой ЭП, в случае размещения ФНС России на своем официальном сайте (www.nalog.ru) в подразделе «Проверь себя и контрагента» раздела «Электронные услуги» сведений о Клиенте об отсутствии связи по указанному адресу (месту нахождения), внесенному в Единый государственный реестр юридических лиц.

6.2.9. Банк отказывает в выполнении распоряжения клиента о совершении операции (за исключением операций по зачислению денежных средств, поступивших на счет Клиента), по которой не представлены документы, необходимые для фиксирования информации в соответствии с положениями Федерального закона № 115-ФЗ от 7 августа 2001 г. «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Федеральный закон № 115-ФЗ), а также в случае если в результате реализации правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма у Банка возникают подозрения, что операция совершается в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма.

6.2.10. В одностороннем порядке приостановить действие или расторгнуть Договор, заблокировать, аннулировать действие Сертификата ключа ЭП/КС КЭП ФНС/Простой ЭП в следующих случаях:

- если Клиент не оплатил комиссионное вознаграждение по Договору в соответствии с Тарифами;

- если у Банка возникают подозрения, что операция Клиента совершается в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма;

- если из общедоступных источников получения информации Банку стало известно, что произошла смена единоличного исполнительного органа, внесена запись о дисквалификации лица, являющегося единоличным исполнительным органом, внесена запись в ЕГРЮЛ/ЕГРИП о прекращении деятельности Клиента;

- если документ удостоверяющий личность владельца Сертификата ЭП/КС КЭП ФНС/Простой ЭП признан недействительным;

- если Клиент после процедуры обновления Сертификата ЭП не предоставил оригинал акта приема-передачи в Банк.

- если от Банка России получена информация, содержащаяся в Базе данных, которая содержит сведения, относящиеся к Клиенту и (или) его электронному средству платежа, на период нахождения указанных сведений в Базе данных.

6.2.11 Банк имеет право выполнять дополнительные проверки электронных документов Клиента, в случаях, установленных действующим законодательством Российской Федерации, отказать Клиенту в совершении операции по переводу денежных средств и/или зачислении денежных средств.

6.3. Клиент имеет право:

6.3.1. Получать от Банка консультации по вопросам использования Системы «Интернет-банк».

6.3.2. В любое время по своему усмотрению инициировать замену ключей и пароля. В этом случае в срок не менее чем за 10 (Десять) календарных дней до предполагаемой замены Клиент обязан уведомить Банк о готовящейся смене ключей или пароля и в течение этого срока обеспечить предоставление в Банк уведомления об изменении параметров подключения.

6.3.3. Приостановить, возобновить, аннулировать действие Сертификата ключа ЭП/КС КЭП ФНС/Простой ЭП, путем направления в Банк соответствующего уведомления.

6.3.4. Клиент, присоединяясь к настоящим Правилам, предоставляет Банку право списывать (в соответствии с Тарифами) на условиях заранее данного акцепта Клиента суммы комиссионного вознаграждения Банка со счетов Клиента, открытых в Банке.

6.3.5. На основании заявления установленной формы, предоставляемого в Банк, устанавливать ограничения по совершаемым операциям по переводу денежных средств по следующим параметрам:

- на максимальную сумму документа;
- на сумму документов за день;
- на перечень возможных получателей денежных средств;
- на перечень идентификаторов устройств (IP адресов), с использованием которых может осуществляться подготовка и (или) подтверждение клиентом электронных сообщений.

6.3.6. На основании заявления установленной формы, предоставляемого в Банк, запросить настройку следующих уведомлений: о входе в Систему «Интернет-банк», об отправке платежей в Банк, об исполнении платежей Банком, а также запросить дополнительный пароль о входе в Систему «Интернет-банк».

6.3.7. В рамках отдельных договоров, соглашений, правил и прочих документов, заключенных между Клиентом и третьими лицами, запросить оформление подтверждающей подписи. Правом подтверждающей подписи наделяются лица, не являющиеся работниками организации, но имеющие полномочия контролировать работу этой организации.

7. Ответственность сторон

7.1. Банк не несет ответственности перед Клиентом за последствия компрометации ключа ЭП/ключа КЭП ФНС/средств Простой ЭП Клиентом или его представителями, а также за убытки, понесенные Клиентом в связи с неправомерными действиями третьих лиц.

7.2. Стороны не отвечают за правильность заполнения и оформления электронных документов другой Стороной.

7.3. Банк не несет ответственности за последствия исполнения электронного документа, защищенного корректной ЭП/КЭП ФНС/Простой ЭП Клиента, в т.ч. в случае использования программно-аппаратных средств клиентской части Системы «Интернет-банк» неуполномоченным лицом.

Банк не несет ответственности в случае реализации угроз несанкционированного доступа неуполномоченных лиц к рабочему месту Системы «Интернет-банк», установленному у Клиента (включая удаленный сетевой доступ), и ключам ЭП/КЭП ФНС/средствам Простой ЭП Клиента, включая угрозы со стороны внутренних (локальных) и внешних (глобальных) сетей связи.

Банк не несет ответственности за несанкционированный доступ третьих лиц к мобильному устройству, SIM-карте, используемым Клиентом для осуществления доступа к счету посредством мобильного приложения Системы «Интернет-банк» с использованием Простой ЭП, до момента получения от Клиента уведомления о несанкционированном доступе третьих лиц к мобильному устройству, SIM-карте либо об утере, повреждении мобильного устройства, SIM-карты. Банк не несет ответственности за неработоспособность оборудования и программных средств Клиента и третьих лиц, повлекшую за собой невозможность доступа Клиента к банковской части Системы «Интернет-банк», и возникшие в результате этого задержки в осуществлении операций Клиента, а также за возможное уничтожение (в полном или частичном объеме) информации, содержащейся на вычислительных средствах Клиента, подключенных к сети «Интернет» для обеспечения предоставления услуг по настоящему Договору.

Банк не несет ответственности за несоответствие реализованного Клиентом или третьими лицами в его программном обеспечении формата обмена актуальному формату, заявленному на сайте <https://orbank.ru>.

7.4. Клиент несет всю ответственность за убытки, возникшие вследствие разглашения или передачи третьей стороне ключей ЭП, ключей КЭП ФНС, средств Простой ЭП. Использование Системы «Интернет-банк», средств дополнительной защиты, ключей ЭП, Сертификатов ЭП, ключей КЭП ФНС, КС КЭП ФНС, средств Простой ЭП не Клиентом либо лицами, не уполномоченными им в установленном порядке, и без предоставления Банку документов, подтверждающих полномочия указанных лиц, в том числе в результате нарушения Клиентом условий Правил, совершение операций без согласия Клиента является нарушением Клиентом порядка использования электронного средства

платежа - Системы «Интернет-банк», в том числе если это повлекло совершение операций без согласия Клиента или его уполномоченных лиц. В этом случае Банк не отвечает за операции, которые совершаются с использованием Системы «Интернет-банк» под видом Клиента.

7.5. Стороны не несут ответственности за действия третьих лиц, предоставляющих услуги связи, в случае невозможности выполнять обмен ЭД/Простых ЭД с помощью Системы «Интернет-банк», платежные документы для исполнения и выписки Клиента представляются на бумажных носителях по адресу Банка, где открыт счет Клиенту.

7.6. Стороны освобождаются от ответственности за полное или частичное неисполнения своих обязательств в соответствии с Договором, если это явилось следствием действия обстоятельств, предвидеть наступление которых и/или предотвратить разумными мерами не было возможности, и которые не зависят от воли Сторон, такие как: стихийные бедствия, пожары, военные действия, массовые беспорядки, бунты, народные волнения, моратории или иные подобные действия органов государственной власти или управления, забастовки работников энергетического комплекса или отрасли связи, отсутствие телефонной связи, отсутствие обеспечения электроэнергией одной из Сторон, аварии телефонного или электрического кабеля и т.п. обстоятельства.

О наступлении и прекращении действия перечисленных в настоящем пункте обстоятельств Сторона, для которой они явились причиной неисполнения обязательств, должна незамедлительно уведомить другую Сторону любым доступным способом, с обязательным дублированием уведомления в письменной форме.

Свидетельство, выданное компетентным государственным органом, будет являться достаточным подтверждением наличия обстоятельств непреодолимой силы.

7.7. Стороны признают, что работа Системы может быть приостановлена без предварительного уведомления Клиентов в случае возникновения необходимости применения мер по управлению информационными и финансовыми рисками, когда непринятие указанных мер может повлечь возникновение угрозы безопасности работы Системы, в том числе угрозу безопасности совершения платежей и/или информационной безопасности. Допускается временное прекращение работы Системы «Интернет-банк» для проведения регламентных, профилактических, иных работ суммарно не более чем на 3 (Три) часа в сутки в рабочие дни и не более чем на 12 (Двенадцать) часов в выходные и праздничные дни. В этом случае Банк не несет ответственности за невозможность использования Системы «Интернет-банк» и за форму совершения платежа.

7.8. Стороны признают, что в соответствии с Федеральным законом № 161-ФЗ «О национальной платежной системе» уведомление об изменении состояния документа, доступное Клиенту для просмотра в Системе «Интернет-банк», является основным способом уведомления Клиента об исполнении распоряжения о переводе денежных средств. В соответствии п. 6.3.6. настоящих Правил по запросу Клиента Банк настраивает отправку уведомлений на электронную почту и/или при помощи SMS-сообщений, оформляется Банком дополнительно по отдельной заявке Клиента.

7.9. Банк не несет ответственности если Клиент по причинам, не зависящим от Банка, несвоевременно получил уведомление и не сообщил в Банк о совершении операции по переводу денежных средств без добровольного согласия Клиента, в том числе если Клиент сменил и/или не сообщил актуальный номер телефона и/или адрес электронной почты.

8. Порядок разрешения споров и конфликтов

8.1. Все разногласия, споры и конфликтные ситуации, возникающие между Сторонами вследствие исполнения Договора, разрешаются с учётом взаимных интересов путём переговоров. На время разрешения спорной ситуации Банк имеет право немедленно приостановить приём/отправку и исполнение электронных документов в одностороннем порядке. В этом случае Банк обязан по Системе «Интернет-банк» или иным способом, определенным Правилами, уведомить Клиента о приостановке его работы в Системе «Интернет-банк».

8.2. В случае возникновения конфликтной ситуации между Банком и Клиентом по предмету Договора, связанной с подлинностью электронных документов, совместным решением обеих Сторон создаётся комиссия. Порядок разрешения споров и конфликтных ситуаций установлен в разделе 3 Приложения № 1 к настоящим Правилам. При решении вопросов по всем остальным конфликтам Стороны руководствуются действующим законодательством Российской Федерации.

8.3. Банк рассматривает заявления Клиента при возникновении споров, связанных с использованием Клиентом, его уполномоченными лицами Системы «Интернет-банк», а также предоставляет Клиенту возможность получать информацию о результатах рассмотрения заявлений (в том числе в письменной форме по требованию Клиента) в срок не более 30 дней со дня получения таких заявлений и не более 60 дней со дня получения заявления Клиента при использовании Системы «Интернет-банк» для осуществления трансграничного перевода денежных средств.

8.4. Споры подлежат рассмотрению в Арбитражном суде Оренбургской области.

9. Срок действия Договора и порядок его расторжения

9.1. Договор действует в течение срока действия Основного(-ых) договора(-ов).

9.2. Любая из Сторон вправе в любое время расторгнуть Договор в одностороннем (внесудебном) порядке, письменно предупредив об этом другую Сторону. До даты расторжения Договора Клиент обязан оплатить задолженность перед Банком, возникшую вследствие исполнения Договора.

9.3. Договор прекращает свое действие с момента расторжения последнего из договоров, заключенных между Клиентом и Банком.

10. Обработка персональных данных

При подписании Заявления о присоединении к Правилам с целью подключения и эксплуатации дистанционного банковского обслуживания в Системе «Интернет-банк»:

1. Единоличный исполнительный орган или Представитель¹ Клиента, наделенный правом заключения/расторжения договоров с Банком по доверенности, дает Банку, в том числе его подразделениям, согласие на обработку своих персональных данных для исполнения ст.9 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – согласие);

Клиент выступает Оператором обработки персональных данных и поручает Банку, в том числе его подразделениям, проводить обработку персональных данных субъектов персональных данных - учредителя (-ей) организации, бенефициарного (-ых) владельца (-ев), выгодоприобретателя (-ей), представителя (-ей), ЕИО, доверительного (-ых) управляющего (-их) долей (-ями) в уставном капитале - на основании ч. 3 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" (далее – поручение).

Под обработкой Банком персональных данных понимаются действия (операции) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, обезличивание, блокирование, удаление, уничтожение, предоставление третьим лицам, действующим на основании агентских договоров или иных договоров, заключенных ими с Банком и содержащих условие об обработке персональных данных в объеме, необходимом для исполнения договора, а также условие о конфиденциальности и неразглашении информации.

Перечень указанных третьих лиц размещен на сайте Банка <https://orbank.ru/> («Перечень третьих лиц, которые осуществляют обработку персональных данных клиентов на основании заключенных ими с Банком договоров») и может быть изменен Банком в связи с заключением/расторжением агентских или иных договоров, заключенных третьими лицами с Банком и содержащих условие об обработке персональных данных, о чем Банк извещает клиента путем обновления информации на сайте Банка.

Банк может проверить достоверность персональных данных, предоставленных единоличным исполнительным органом или Представителем Клиента, наделенным правом заключения/расторжения договоров с Банком по доверенности, а также персональных данных субъектов персональных данных, указанных выше по тексту, используя информационные ресурсы других операторов.

Под персональными данными понимается информация, относящаяся к субъекту персональных данных: фамилия, имя, отчество, дата и место рождения, реквизиты документа, удостоверяющего личность, ИНН, адрес, телефон, электронный адрес, сведения, характеризующие соблюдение законодательства Российской Федерации, сведения, полученные от третьих лиц, в том числе государственных органов, государственных информационных систем, единой системы идентификации и аутентификации (ЕСИА), Фонда пенсионного и социального страхования Российской Федерации, сведения, полученные через систему межведомственного электронного взаимодействия (СМЭВ), и/или из сети Интернет, и/или из иных общедоступных источников персональных данных.

Согласие и/или поручение на обработку персональных данных может быть отозвано, если иное не установлено законодательством РФ, по обращению в Банк / к третьему лицу (в любой форме, позволяющей подтвердить факт получения Банком/третьим лицом отзыва):

- субъекта персональных данных – для отзыва согласия на обработку персональных данных;
- Клиента, выступающего Оператором обработки персональных данных – для отзыва поручения.

В случае отзыва согласия и/или поручения Банк/третье лицо (если исполнение заключенного договора с Банком предполагает передачу третьим лицам персональных данных) имеет право продолжить обработку персональных данных на основаниях, предусмотренных действующим законодательством РФ².

2. Клиент в лице представителя, наделенного правом заключения/расторжения договоров с Банком от имени и в интересах Клиента, выступая Оператором обработки персональных данных, гарантирует:

- наличие согласия субъекта персональных данных на их обработку Банком. Банк не обязан

¹ Представитель – лицо, действующее от имени и в интересах клиента, полномочия которого основаны на доверенности, договоре.

² Банк продолжает обработку персональных данных, например, когда обработка персональных данных необходима для исполнения требования налогового, банковского законодательства, нормативных актов Банка России.

получать отдельное согласие субъектов персональных данных на обработку их персональных данных;

- хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше чем этого требуют цели обработки персональных данных, в том числе по настоящему поручению;

- обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки в рамках настоящего поручения или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных";

- своевременное доведение до Банка информации в случае отзыва субъектом персональных данных согласия на обработку его персональных данных;

- своевременное доведение до субъектов персональных данных информации о перечне третьих лиц, которым Банк предоставляет персональные данные субъекта в рамках агентских договоров или иных договоров, заключенных ими с Банком и содержащих условие об обработке персональных данных в объеме, необходимом для исполнения договора, а также условие о конфиденциальности и неразглашении информации. Банк обязан обеспечить актуальность перечня третьих лиц на сайте Банка <http://orbank.ru>".

3. В случае обращения к Банку субъекта персональных данных с запросом, основанным на ст. 14 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных", Банк информирует об этом Оператора обработки персональных данных и действует в соответствии с его инструкциями.

4. Ответственность перед субъектом персональных данных за действия Банка несет Оператор обработки персональных данных.

5. Банк обязан:

- при обработке персональных данных принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

- при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет" обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации;

- принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами. Банк самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных" или другими федеральными законами.

- по запросу Оператора обработки персональных данных предоставлять в течение срока действия поручения Оператора, в том числе до обработки персональных данных, информацию о соблюдении условий обработки персональных данных;

- соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при выполнении поручения;

- в случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных при обработке персональных данных Банком, повлекшей нарушение прав субъектов персональных данных, Банк обязан уведомить Оператора обработки персональных данных в соответствии со ст. 21 ч. 3.1. Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента по Системе "Интернет-Банк "Faktura.ru" (при действующем договоре) или заказным письмом.

6. Согласие и/или поручение вступает в силу со дня его подписания и действует до полного исполнения обязательств по договору(-ам). Банк имеет право прекратить обработку предоставленных персональных данных в любой момент до окончания указанного срока.

В случае отказа клиента выступать Оператором обработки персональных данных субъекты персональных данных, указанные в п.1 настоящего раздела, предоставляют в Банк (каждый индивидуально) согласие на обработку персональных данных, оформленное по типовой форме Банка.

11. Прочие условия

11.1. Банк вправе вносить изменения в настоящие Правила, с предварительным извещением

Клиента не менее чем за 10 (Десять) календарных дней до даты вступления изменений в силу.

Введение новых услуг и продуктов Банка, изменение в законодательные акты РФ, в Правила сервиса «ФАКТУРА.RU», Правила электронного документооборота корпоративной информационной системы «BeSafe, в Правила работы Удостоверяющего Центра «AUTHORITY (если такое введение не является видоизменением уже действующих отношений с Клиентами) не требует предварительного уведомления за 10 (Десять) календарных дней. Информация об изменениях, вносимых в настоящие Правила, доводится до сведения Клиента путем ее размещения в операционных залах Банка и на web-сайте Банка по адресу <https://orbank.ru>.

11.2. В случае изменения законодательства Российской Федерации настоящие Правила применяются в части, не противоречащей вновь принятым нормативным актам.

11.3. В случае несогласия Клиента с изменениями, внесенными в настоящие Правила, Клиент вправе расторгнуть Договор, предоставив в Банк Заявление до вступления в силу таких изменений.

11.4. В случае если до вступления в силу опубликованных Банком изменений, внесенных в настоящие Правила, Банк не получил от Клиента Заявление о расторжении Договора, Стороны признают, что указанные изменения приняты Клиентом.

11.5. Банк не несет ответственности, если информация об изменении настоящих Правил, изменении Тарифов Банка, опубликованная в порядке и в сроки, установленные настоящими Правилами, не была получена и/или изучена, и/или правильно истолкована Клиентом.

1. Список электронных документов

Основанием для возникновения обязательств Сторон в рамках Договора является передача в Системе «Интернет-банк» следующих электронных документов:

- платежное поручение;
- распоряжение на обязательную продажу валюты;
- поручение на продажу валюты;
- поручение на покупку валюты;
- заявление на перевод валюты;
- заявление на отзыв документа;
- справка о подтверждающих документах;
- документ свободного формата;
- запрос на выписку;
- выписка по счету;
- сведения о валютных операциях;
- заявление о регистрации контракта (кредитного договора);
- заявление о внесении изменений в контракт (кредитный договор);
- заявление о снятии с учета контракта (кредитного договора);
- иные электронные документы, которые могут быть разработаны Банком, введены действующим законодательством и будут использоваться в работе Банка и Клиента.

Требования по оформлению вышеперечисленных электронных документов регламентируются нормативными документами Банка России.

2. Способы передачи и регламент приема в Системе «Интернет-банк»

2.1. График приёма и обработки электронных документов.

Банк принимает ЭД/Простые ЭД/ ДСФ от Клиента ежедневно, за исключением выходных и праздничных дней, с 09:00 до 19:00 (предпраздничные дни до 18:00).

Банк производит исполнение документов в соответствии с Договорами.

На дату утверждения настоящих Правил Банком установлено следующее операционное время:

- прием расчетных документов в валюте Российской Федерации по Системе «Интернет-банк» осуществляется ежедневно, кроме выходных и праздничных дней, с 09:00 часов до 19:00 часов, в предпраздничные дни с 09:00 часов до 18:00 часов;
- прием расчетных документов в иностранной валюте по Системе «Интернет-банк» осуществляется ежедневно, кроме выходных и праздничных дней, с 09:00 часов до 17:00 часов, в предпраздничные дни с 09:00 часов до 16:00 часов.

Платежные документы, принятые Банком после операционного времени, исполняются не позже рабочего дня, следующего за днём их получения от Клиента.

2.2. Работа Клиента в Системе «Интернет-банк» состоит из следующих основных этапов:

- вход в сервис для получения выписки;
 - контроль остатка по счету и состояния документов, обработанных Банком;
 - заполнение электронных бланков документов, подпись платежных документов должностными лицами с правом подписи ЭД/Простых ЭД/ ДСФ;
 - отправка ЭД/Простых ЭД/ ДСФ в Банк;
 - контроль доставки ЭД/Простых ЭД/ ДСФ в Банк;
 - контроль обработки ЭД/Простых ЭД/ ДСФ Банком;
 - в случае отрицательных результатов обработки ЭД/Простых ЭД/ ДСФ – анализ причин отказа, уточнение и получение телефонных консультаций при возникновении сомнений в правомерности возврата документов;
 - исправленные документы могут быть отправлены в Банк в соответствии с графиком приема ЭД/Простых ЭД/ ДСФ;
 - при необходимости Клиент отправляет в Банк заявку на отзыв ЭД/Простых ЭД/ ДСФ.
- Исполнение ЭД/Простых ЭД может быть отменено в том случае, если соответствующая сумма не была списана Банком с корреспондентского счета Банка.

2.3. Порядок подключения Клиента к Системе «Интернет-банк»

2.3.1. Для подключения к Системе «Интернет-банк» с использованием Ключей ЭП Клиент представляет уполномоченному работнику Банка подписанное со своей стороны Заявление о присоединении к Правилам (Приложение № 3 к настоящим Правилам) и Заявление на выдачу

сертификата ключа проверки ЭП (Приложение № 4 к настоящим Правилам) – для представителя юридического лица, действующего от имени юридического лица без доверенности, Заявление на выдачу сертификата ключа проверки ЭП (Приложение № 6) – для физического лица (уполномоченного лица Клиента). При оформлении Заявлений необходимо учитывать, что лица, которым предоставляется право подписи ЭД, должны быть указаны в карточке с образцами подписей и оттиска печати, за исключением лиц, которым в соответствии с п. 6.3.7. настоящих Правил предоставлена подтверждающая подпись.

2.3.2. Для подключения к Системе «Интернет-банк», с использованием Простой ЭП, Клиент представляет уполномоченному работнику Банка подписанное со своей стороны Заявление о присоединении к Правилам (Приложение № 3 к настоящим Правилам) и Заявление на выдачу Логина и Пароля (Приложение № 5 к настоящим Правилам). При оформлении Заявлений необходимо учитывать, что лица, которым предоставляется право подписи Простых ЭД, должны быть указаны в карточке с образцами подписей и оттиска печати, за исключением лиц, которым в соответствии с п. 6.3.7. настоящих Правил предоставлена подтверждающая подпись.

2.3.3. Для подключения к Системе «Интернет-банк» с использованием Ключей КЭП ФНС Клиент представляет уполномоченному работнику Банка подписанное со своей стороны Заявление о присоединении к Правилам (Приложение № 3 к настоящим Правилам). При оформлении Заявления необходимо учитывать, что лица, которым предоставляется право подписи ЭД, должны быть указаны в карточке с образцами подписей и оттиска печати, за исключением лиц, которым в соответствии с п. 6.3.7. настоящих Правил предоставлена подтверждающая подпись.

2.3.4. Клиент обеспечивает наличие денежных средств на расчетном счете для оплаты комиссии в размере, установленным Тарифами, Банк производит оплату за регистрацию ключевой информации в Системе «Интернет-банк» в соответствии с Тарифами.

2.3.5. При подключении с использованием Ключей ЭП в течение 5 (пяти) рабочих дней уполномоченный работник Банка регистрирует договор в Системе «Интернет-банк». После регистрации уполномоченный работник Банка передает Клиенту (уполномоченному лицу Клиента) Сертификат ключа проверки электронной подписи. Передача оформляется актом приема-передачи (Форма определена Правилами работы Удостоверяющего Центра «AUTHORITY»), после подписания Владелец сертификата Банк регистрирует права Владельца Сертификата в Сервисе. После регистрации прав Клиент вправе осуществлять операции с использованием данного Сертификата в Сервисе.

2.3.6. При подключении с использованием Простой ЭП в течение 5 (пяти) рабочих дней уполномоченный работник Банка регистрирует договор в Системе «Интернет-банк». После регистрации уполномоченный работник Банка осуществляет отправку Логина на адрес электронной почты, указанной в заявлении на выдачу Логина и Пароля (Приложение № 5 к настоящим Правилам), осуществляет отправку Пароля на номер телефона для получения разовых паролей, указанного в заявлении на выдачу Логина и Пароля (Приложение № 5 к настоящим Правилам). После отправки Логина и Пароля Банк регистрирует права владельца Логина в Сервисе. После регистрации прав Клиент вправе осуществлять операции с использованием данного Логина в Сервисе.

2.3.7. При подключении Клиента к Системе «Интернет-банк», с использованием КЭП ФНС в течение 5 (пяти) рабочих дней уполномоченный работник Банка регистрирует договор в Системе «Интернет-банк». После регистрации уполномоченный работник Банка на адрес электронной почты, указанной в Заявлении о присоединении к Правилам (Приложение № 3 к настоящим Правилам) осуществляет отправку ссылки на регистрацию КС КЭП ФНС, после успешной регистрации сертификата Банк получает запрос, после обработки запроса и регистрации прав Клиент вправе осуществлять операции с использованием данного Сертификата в Сервисе.

2.4. Изменение параметров подключения к Системе «Интернет-банк»

2.4.1. При необходимости изменения параметров подключения к Системе «Интернет-банк» или изменении состава Владелец сертификатов ключей ЭП, владельцев Простой ЭП, Клиент направляет в Банк Заявление на внесение изменений в Систему «Интернет-банк» (Приложение № 7 к настоящим Правилам), Заявление на выдачу сертификата ключа проверки ЭП (Приложения № 4/№ 6 к настоящим Правилам) и/или Заявление на выдачу Логина и Пароля (Приложение № 5 к настоящим Правилам). При изменении параметров подключения к Системе «Интернет-банк» или изменении состава Владелец КС КЭП ФНС, Клиент направляет в Банк Заявление на внесение изменений в Систему «Интернет-банк» (Приложение № 7 к настоящим Правилам). Значения ранее установленных параметров утрачивают силу. Заявление на внесение изменений в Систему «Интернет-банк» не является основанием для прекращения действия Договора.

2.4.2. При изменении состава владельцев сертификатов ключей ЭП, владельцев КС КЭП ФНС, владельцев Простой ЭП на период ввода в действие новых параметров подключения, указанных в Заявлении, возможно возникновение ситуации отказа в обработке ЭД/Простых ЭД/ ДСФ. Для исключения отказа в обработке ЭД/Простых ЭД Клиент должен заблаговременно отослать в Банк все подписанные ЭД/Простые ЭД/ ДСФ, а непосредственно перед началом периода ввода в действие новых

параметров подключения получить из Банка подготовленные в его адрес ЭД.

2.4.3. Процедура ввода в действие новых параметров подключения производится аналогично процедуре подключения Клиента к Системе, описанной в п. 2.3.4, 2.3.5., 2.3.6., 2.3.7., настоящего Приложения.

2.5. Порядок проведения плановой смены ключей ЭП.

2.5.1. Срок действия Сертификата ключа подписи составляет один календарный год с момента генерации Сертификата. Продление срока действия Сертификата ключа подписи на новый срок оформляется обязательной сменой ключей не позднее 10 дней до момента окончания срока действия Сертификата.

2.5.2. За 14 дней до истечения срока действия ключа ЭП Система «Интернет-банк» начинает при каждой загрузке напоминать владельцу сертификата ключа ЭП о необходимости произвести смену ключа. Банк по Системе «Интернет-банк» отправляет Клиенту сообщение, содержащие порядок процедуры обновления действующего сертификата ключа ЭП. Клиент обязуется подписать электронный акт приема-передачи действующим ключом и предоставить акт приема-передачи в Банк в распечатанном и подписанном виде.

2.5.3. Продление сертификата возможно при условии, что действие сертификата еще не закончилось. После окончания срока действующих ключей ЭП оформление новых сертификатов ключей ЭП производится в обычном порядке в соответствии с п. 2.4. настоящего Приложения.

2.5.4. Для КС КЭП ФНС сроки и процедура смены устанавливается регламентом УЦ ФНС и контролируется Клиентом самостоятельно.

2.6. Порядок действий в случае компрометации ключей ЭП/КЭП ФНС/Простой ЭП.

2.6.1. Решение о компрометации ключа ЭП может быть принято владельцем сертификата ключа ЭП, владельцем КС КЭП ФНС, владельцем Простой ЭП, руководством Клиента или Банком.

2.6.2. Работа на скомпрометированном ключе ЭП/Простой ЭП должна быть приостановлена. О компрометации ключа ЭП/ключа КЭП ФНС/средств Простой ЭП Клиент незамедлительно уведомляет Банк по телефону (3532) 343-191, 343-171.

При обращении Клиенту необходимо сообщить следующие сведения:

- название, ИНН – для юридических лиц, ФИО, ИНН – для индивидуальных предпринимателей и физических лиц, занимающихся в установленном порядке Российской Федерации частной практикой;
- ФИО владельца ключа.

Уведомление принимается и обрабатывается ежедневно, за исключением выходных и праздничных дней, с 09:00 до 17:00 (предпраздничные дни до 16:00).

Если сведения о компрометации ключа ЭП/ключа КЭП ФНС/средств Простой ЭП, Клиента стали известны в период времени, когда заявки по телефону Банком не обрабатываются, Клиенту необходимо уведомить Банк по телефону в начале следующего рабочего периода. После передачи уведомления Клиент должен зафиксировать ФИО работника Банка, который принял уведомление, а также дату и время передачи уведомления.

В срок не позднее следующего дня Клиент направляет в Банк уведомление о компрометации в письменной форме. Уведомление принимается Банком к исполнению только от должностных лиц Клиента, имеющих право подписи, и представителей Клиента, действующих на основании надлежащим образом оформленной доверенности.

2.6.3. Получив предварительное сообщение о компрометации ключевой информации, Банк приостанавливает обработку ЭД/Простых ЭД, подписанных на предположительно скомпрометированным ключом ЭП/КЭП ФНС/Простой ЭП до получения уведомления в письменной форме. После получения уведомления в письменной форме Банк отзывает сертификат скомпрометированного ключа ЭП путем помещения его в список отозванных сертификатов. В случае компрометации ключа КЭП ФНС блокировка самого сертификата находится в компетенции УЦ ФНС, Сервис осуществляет отзыв прав доступа для скомпрометированного ключа только на уровне прав КС КЭП ФНС. Если поступило сообщение о компрометации средств Простой ЭП, Банк блокирует Логин. Подключение новых владельцев сертификатов ключей ЭП, владельцев Простой ЭП производится в обычном порядке в соответствии с п. 2.4. настоящего Приложения.

2.7. Порядок осуществления переводов денежных средств по распоряжению Клиента в рамках исполнения Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе», поступивших по Системе Интернет-банк FAKTURA.RU

2.7.1. Перевод денежных средств по распоряжению Клиента без использования Системы быстрых платежей.

В соответствии с требованиями Федерального закона от 27.06.2011г. № 161-ФЗ «О национальной платежной системе» Банк при выявлении перевода, совершаемого без добровольного согласия³ Клиента, обязан приостановить прием к исполнению распоряжения Клиента на 2 (Два) дня.

При этом с Клиентом осуществляется взаимодействие одним из следующих способов: непосредственно Банком либо Оператором сервиса от имени Банка.

1. **Банк** в лице уполномоченного работника проводит работу с Клиентом в соответствии с порядком, установленным в п. 8.1.16 Условий открытия и ведения банковского счета юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся частной практикой в АО «БАНК ОРЕНБУРГ» (в валюте РФ).

2. Оператор сервиса от имени Банка:

2.1. На контактный номер телефона отправляет SMS-сообщение о приостановлении приема к исполнению распоряжения Клиента по форме, установленной Оператором сервиса с учетом требований ст. 8 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе».

2.2. Связывается с Клиентом по контактному номеру телефона для получения от Клиента подтверждения операции, производит запись телефонного разговора с Клиентом, обеспечивает хранение записи телефонного разговора на защищенных носителях информации в течение 3 (трех) лет.

2.2.1. Распоряжение Клиента признается не принятым к исполнению:

✓ При невозможности связаться с Клиентом в целях получения подтверждения операции, либо при не получении Оператором сервиса/Банком от Клиента подтверждения операции до конца календарного дня, следующего за днем отправки Клиентом распоряжения.

✓ При получении от Клиента отказа от совершения операции либо, если физическим лицом, с которым связался Оператор сервиса по контактному номеру телефона, не пройдена процедура идентификации в качестве Клиента; либо при отказе физическим лицом, с которым Оператор сервиса связался по контактному номеру телефона, от прохождения процедуры идентификации.

✓ При получении от Клиента подтверждения операции, но в случае отказа Клиентом от приемки к исполнению такого распоряжения Банком.

2.2.2. При получении Оператором сервиса/Банком от Клиента подтверждения операции распоряжение незамедлительно проверяется на наличие совпадений со сведениями из Базы данных.

Если при проверке на наличие совпадений со сведениями из Базы данных выявляется совпадение информации о получателе денежных средств, либо о параметре устройства, с использованием которого Клиент прошел авторизацию, с информацией из Базы данных, то:

- распоряжение приостанавливается на два дня со дня предоставления Клиентом подтверждения платежа;

- Клиенту на контактный номер телефона Оператором сервиса отправляется SMS-сообщение о приостановлении подтвержденного распоряжения Клиента по форме, установленной Оператором сервиса с учетом требований ст. 8 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе»;

- по истечении двух дней со дня предоставления Клиентом подтверждения, распоряжение принимается к исполнению Банком.

Если при проверке на наличие совпадений со сведениями из Базы данных, не обнаруживается совпадений информации о получателе денежных средств или о параметре устройства, с использованием которого Клиент прошел авторизацию, с информацией из Базы данных, то распоряжение незамедлительно принимается к исполнению Банком.

Подтверждение Клиентом распоряжения может быть предоставлено Оператору сервиса в процессе телефонного разговора, непосредственно в Банк на бумажном носителе и/или по Системе Интернет-банк FAKTURA.RU в установленные законодательством сроки. Приоритет используемого способа уведомления Клиента и получения подтверждения платежа устанавливается Банком.

Если последний день срока приходится на нерабочий день, днем окончания срока считается ближайший следующий за ним рабочий день (ст. 193 ГК РФ).

³ Перевод денежных средств без добровольного согласия Клиента – перевод без согласия Клиента или с согласия Клиента, полученного под влиянием обмана или при злоупотреблении доверием. Признаки осуществления перевода денежных средств без добровольного согласия Клиента устанавливаются Банком России и размещаются на его официальном сайте в информационно-телекоммуникационной сети "Интернет".

2.7.2. Перевод денежных средств по распоряжению Клиента с использованием Системы быстрых платежей (СБП)

В соответствии с требованиями Федерального закона от 27.06.2011г. № 161-ФЗ «О национальной платежной системе» Банк при выявлении перевода, совершаемого без добровольного согласия Клиента, обязан отказать Клиенту в совершении операции.

1. При этом Оператор сервиса от имени Банка доводит информацию до Клиента посредством SMS-сообщения и телефонного звонка на контактный номер телефона в соответствии с требованиями ст. 8 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе».

- об отказе в совершении операции (перевода) в связи с выявлением операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента;

- о рекомендациях по снижению рисков повторного осуществления перевода денежных средств без добровольного согласия Клиента;

- о возможности Клиента совершить повторную операцию, содержащую те же реквизиты получателя (плательщика) и ту же сумму перевода (далее - повторная операция).

При этом Оператор сервиса производит запись телефонного разговора с Клиентом, обеспечивает хранение записи телефонного разговора на защищенных носителях информации в течение 3 (трех) лет.

Распоряжение Клиента признается не принятым к исполнению:

- ✓ При получении от Клиента опровержения операции; либо если физическим лицом, с которым Банк/Оператор сервиса связался по контактному номеру телефона, не пройдена процедура идентификации в качестве Клиента; либо при отказе физическим лицом, с которым Оператор сервиса связался по контактному номеру телефона, от прохождения процедуры идентификации.

- ✓ При получении Оператором сервиса подтверждения по осуществлению действий по совершению операции, но в случае несогласия Клиента с исполнением такого распоряжения по СБП.

- ✓ При невозможности связаться с Клиентом.

2. При получении Оператором сервиса от Клиента согласия Клиента на возобновление Банком приема к исполнению распоряжения по СБП, Оператор сервиса предоставляет Клиенту возможность подписания и отправки Банку повторного перевода.

Если Клиент совершил повторный перевод, он незамедлительно проверяется Оператором сервиса на наличие совпадений со сведениями из Базы данных.

2.1. При наличии совпадений о получателе денежных средств, либо о параметре устройства, с использованием которого Клиент прошел авторизацию, со сведениями из Базы данных:

- Клиенту на контактный номер телефона Оператором сервиса от имени Банка отправляется уведомление путем SMS-сообщения об отказе в совершении Клиентом повторной операции с указанием причины и срока отказа, а также о возможности совершения Клиентом последующей повторной операции по истечении двух дней со дня совершения повторной операции.

- По истечении двух дней со дня совершения повторной операции, последующий повторный перевод незамедлительно будет принят к исполнению Банком.

2.2. Если при проверке на наличие совпадений со сведениями из Базы данных не обнаруживается совпадений информации о получателе денежных средств или о параметре устройства, с использованием которого Клиент прошел авторизацию, с информацией из Базы данных, то повторный перевод незамедлительно будет принят к исполнению Банком.

Если последний день срока приходится на нерабочий день, днем окончания срока считается ближайший следующий за ним рабочий день (ст. 193 ГК РФ).

Приостановление приема к исполнению распоряжения Клиента/отказе в исполнении не распространяется на случаи осуществления переводов денежных средств, являющихся заработной платой и (или) иными доходами, в отношении которых статьей 99 Федерального закона от 2 октября 2007 года N 229-ФЗ "Об исполнительном производстве" установлены ограничения размеров удержания, а также переводов денежных средств, являющихся доходами, на которые в соответствии со статьей 101 Федерального закона от 2 октября 2007 года N 229-ФЗ "Об исполнительном производстве" не может быть обращено взыскание.

При наличии Клиента/электронного средства платежа в Базе данных, Клиент вправе подать в порядке, установленном Банком России, заявление, в том числе через Банк, об исключении сведений, относящихся к Клиенту, из Базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента в соответствии с Указанием Банка России № 6748-У от 13.06.2024.

В случае, если Банк исполняет распоряжение Клиента в нарушение требований, установленных ст. 8 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе», Банк обязан возместить Клиенту сумму операции, о которой Клиент не был проинформирован и которая была

совершена без добровольного согласия Клиента, в течение 30 дней после получения заявления Клиента о возмещении суммы операции, совершенной без добровольного согласия Клиента.

3. Порядок разрешения споров и конфликтных ситуаций.

3.1. В процессе осуществления электронного документооборота между Банком и Клиентом возможно возникновение споров и конфликтных ситуаций, связанных с формированием, доставкой, получением и исполнением электронных документов, а также ситуаций, связанных с функционированием Сервиса. Любые споры в отношении авторства и/или подлинности документа, переданного с использованием Системы «Интернет-банк», подписанного ключом ЭП/КЭП ФНС/Простой ЭП и предназначенного для проверки Сертификатом, зарегистрированным в Системе «Интернет-банк», разрешаются между Сторонами путем проведения переговоров.

3.2. При невозможности разрешения спора путем переговоров Клиент представляет Банку уведомление, содержащее существо претензии с указанием на ЭД/Простой ЭД, на основании которого Банк выполнил операцию по счёту Клиента.

3.3. При получении от Клиента уведомления о возникновении конфликтной ситуации Банк проверяет наличие обстоятельств, свидетельствующих о возникновении конфликтной ситуации, и в срок не позднее 3 (трех) рабочих дней, следующих за датой получения уведомления, направляет Клиенту информацию о результатах проверки и, в случае необходимости, о мерах, принятых для разрешения возникшей конфликтной ситуации.

3.4. Конфликтная ситуация считается урегулированной в рабочем порядке, если Клиент удовлетворен информацией, полученной от Банка.

3.5. В случае если Клиент не удовлетворен информацией, полученной от Банка, для рассмотрения конфликтной ситуации формируется техническая комиссия. Формирование технической комиссии, ее состав, компетенция и полномочия технической комиссии, протокол работы технической комиссии, акт по итогам работы технической комиссии определяется правилами электронного документооборота корпоративной информационной системы «BeSafe».

3.6. Если по результатам работы технической комиссии Стороны не достигли договоренности либо одна из Сторон не согласна с выводами технической комиссии, дальнейшее разбирательство спора продолжается в установленном действующим законодательством РФ порядке.

3.7. Банк несет ответственность перед Клиентом в случае, когда имела место хотя бы одна из следующих ситуаций:

- Банк не предъявляет ЭД/Простой ЭД, переданный Клиентом, на основании которого Банк выполнил операцию по счёту Клиента;

- хотя бы одна из ЭП/КЭП ФНС/Простая ЭП Клиента в оспариваемом ЭД/Простом ЭД оказалась некорректной;

- клиент предоставляет уведомление об компрометации секретного ключа/КЭП ФНС/Простой ЭП с отметкой Банка о принятии, при этом в уведомлении указаны дата и время наступившие ранее даты и времени, указанных в ЭД/Простых ЭД.

3.8. В случае, когда Банк предъявляет ЭД/Простой ЭД, в котором корректность ЭП/КЭП ФНС/Простая ЭП Клиента признана технической комиссией и принадлежность Клиенту ключа ЭП/КЭП ФНС/Простой ЭП подтверждена, Банк перед Клиентом по выполненным на основании спорного ЭД/Простого ЭД операциям ответственности не несет.

РЕГЛАМЕНТ
использования мер безопасности при применении
Системы «Интернет-банк»

Стороны согласились применять настоящий Регламент использования мер безопасности при применении Системы «Интернет-банк», а именно:

- исключить возможность неправомерного получения персональной информации пользователей Системы «Интернет-банк» (не передавать такую информацию другим лицам);
- обеспечить безопасное хранение ключей ЭП на Смарт-карте в сейфе или запираемом металлическом шкафу и т. п.;
- исключить использование Системы «Интернет-банк» и подготовку платежных документов на компьютерах, находящихся в общем доступе (в т. ч. Интернет-кафе, бесплатный Wi-Fi и пр.);
- вставлять Смарт-карту только в момент подписания документов, не оставлять ключи ЭП постоянно подключенными к компьютеру;
- ограничить доступ к своему компьютеру (в том числе и по локальной сети), используемому для работы с Системой «Интернет-банк», обеспечить безопасность помещения, в котором он установлен;
- осуществлять постоянный контроль за отправляемыми платежными документами при работе с Системой «Интернет-банк», а также состоянием своего счета;
- регулярно, не реже одного раза в 45 дней, производить смену PIN кодов для доступа на Смарт-карту;
- в обязательном порядке производить регенерацию ключей ЭП и смену паролей в следующих случаях:
 - 1) при смене ответственных лиц, имеющих право использования Системы «Интернет-банк»;
 - 2) при обнаружении фактов доступа неуполномоченных лиц к ключевой информации (а также при подозрении о таком доступе, в том числе и удаленном доступе по сети);
- обеспечить защиту компьютера, с которого выполняется работа с Системой «Интернет-банк», желательно исключить доступ с этого компьютера в сеть «Интернет», за исключением адресов Системы «Интернет-банк»;
- установить антивирусную программу и регулярно обновлять антивирусную базу;
- обеспечить защиту компьютера от несанкционированного доступа – путём настройки политики безопасности, обеспечения своевременной установки обновлений безопасности операционной системы и прикладных программ;
- использовать только лицензионное программное обеспечение, полученное из надежных источников и необходимое для работы на компьютере с Системой «Интернет-банк»;
- устанавливать все официальные обновления к используемой операционной системе;
- при работе с электронной почтой обращать особое внимание на отправителя сообщения. Если отправитель неизвестен - открывать вложения и иные присланные файлы категорически не рекомендуется, что бы ни было написано в тексте сообщения. Сервисами обмена мгновенными сообщениями (ICQ, Skype, Mail.Ru-Агент и т.п.) на данном компьютере желательно не пользоваться;
- не устанавливать и не сохранять подозрительные файлы, полученные из ненадежных источников, скачанные с неизвестных web-сайтов, присланные по электронной почте и т.д. В случае необходимости загрузки файла обязательно проверьте его антивирусом перед использованием;
- не отвечать на подозрительные письма с просьбой выслать закрытый ключ ЭП, пароль и другие конфиденциальные данные. Подобное письмо гарантированно создано злоумышленниками. Банк ни при каких обстоятельствах и ни в какой форме не запрашивает у клиентов конфиденциальную информацию о закрытых ключах и паролях;
- настроить сервис e-mail или sms-уведомлений об отправке и исполнении платежных документов по своим счетам, а также обо всех своих входах в Систему «Интернет-банк»;
- обращать внимание на дату и время последнего входа в систему (данные фиксируется в журнале сеансов работы после входа в систему).

При использовании мобильного приложения рекомендуется:

- производить установку приложения только из авторизованного магазина приложений (Google Play, App Store);
- установить код доступа на ваше мобильное устройство;
- установить и своевременно обновлять лицензионные антивирусные программы на вашем мобильном устройстве;
- всегда совершать выход из приложения с помощью пункта меню «Выйти»;
- не хранить логин и пароль для доступа, а также код доступа в приложение на своём мобильном устройстве или в общедоступном месте, не записывать его на бумагу;
- ни при каких обстоятельствах не сообщать никому (в том числе работникам банка, родственникам и друзьям) логин, пароль и код доступа в приложение;
- никогда не отвечать на электронные письма, входящие звонки, SMS-сообщения, письменные/устные обращения, в которых запрашиваются коды доступа, разовые пароли, персональная конфиденциальная информация;
- обеспечить конфиденциальность разовых паролей, поступающих на мобильное устройство, не передавать используемое мобильное устройство третьим лицам, а также своевременно блокировать номер телефона в случае утери устройства, SIM-карты;
- сверять текст Разового пароля с реквизитами подтверждаемого Простого ЭД, не использовать Разовый пароль и никому его не сообщать в случае несовпадения;
- не регистрировать номер мобильного телефона, на который приходят Разовые пароли, в социальных сетях и других открытых источниках.

**Заявление о присоединении к Правилам подключения и эксплуатации систем дистанционного
банковского обслуживания в Системе «Интернет-банк»**

Настоящим заявлением Клиент:

Полное наименование Клиента	
ИНН/ОГРН/ОГРНИП	
в лице (должность Ф. И. О. полностью)	
действующего на основании	☐ Устава ☐ Свидательства ☐ Доверенности №__ от «__» _____ 20__ г.
Юридический адрес	
Телефон, e-mail	

1. в соответствии со статьей 428 Гражданского кодекса Российской Федерации, полностью и безусловно присоединяется к действующей редакции Правил подключения и эксплуатации дистанционного банковского обслуживания в Системе «Интернет-банк» для юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой (далее – Правила) и обязуется соблюдать требования Правил со дня принятия настоящего Заявления о присоединении к Правилам АО «БАНК ОРЕНБУРГ» (далее – Банк). Подписание настоящего Заявления о присоединении к Правилам является подтверждением того, что Клиент ознакомлен и согласен с требованиями Правил, действующими на дату подписания, их содержание ему полностью понятно. Правила и Тарифы комиссионного вознаграждения на услуги АО «БАНК ОРЕНБУРГ» юридическим лицам, индивидуальным предпринимателям, физическим лицам, занимающихся частной практикой являются неотъемлемой частью настоящего Заявления о присоединении к Правилам и размещены на web-сайте Банка в сети «Интернет» по адресу <https://orbank.ru>, Тарифы на информационных стендах в подразделении Банка;

2. ознакомлен и согласен с Правилами документооборота корпоративной информационной системы «BeSafe», Правилами сервиса «ФАКТУРА.RU», Правилами работы Удостоверяющего Центра «AUTHORITY», техническими требованиями к оборудованию рабочего места, а также с правом Банка на одностороннее изменение Тарифов;

3. проинформирован Банком об условиях безопасного использования Системы «Интернет-банк», в частности о любых ограничениях способов и мест использования, случаях повышенного риска использования Системы «Интернет-банк»;

4. признает, что получение Банком ЭД/Простого ЭД, подписанного ЭП/КЭП ФНС/Простой ЭП Клиента, юридически эквивалентно получению Банком документа на бумажном носителе, заверенного собственноручными подписями Клиента и оттиском печати;

5. осознаёт, что ответственность за совершение с использованием Системы «Интернет-банк» операций неуполномоченными лицами, в том числе в связи с получением доступа к Системе «Интернет-банк» ключам ЭП/КЭП ФНС/средствам Простой ЭП, сертификатам ключей ЭП/КС КЭП ФНС/Простой ЭП) полностью лежит на Клиенте;

6. заявляет Банку следующий список разрешенных IP-адресов, используемых в рамках работы с Системой «Интернет-банк»:

_____ ;
(перечень адресов / нет)

7. соглашается, что с момента подписания настоящего Заявления действие всех ранее подписанных договоров, определяющих электронный документооборот, прекращается. Ранее выданные по Акту приема-передачи Сертификаты Электронной подписи продолжают свое действие;⁴

8. просит предоставить доступ к Системе «Интернет-банк» уполномоченным лицам с правами для выполнения операций по счетам, указанных в настоящем Заявлении с использованием:

⁴ Данный пункт распространяет свое действие на Клиентов, заключивших ранее с Банком договоры об обмене электронными документами.

(наименование организации, Ф. И. О. Индивидуального предпринимателя/ИНН) ⁵

№	Номер счета	Уполномоченные лица (должность Ф. И. О. полностью) ⁶	Разрешено запрашивать выписку (да/нет)	Разрешено создавать платежные документы (да/нет)	Разрешено подписывать и отправлять документы (да/нет)	Тип подписи (первая/ вторая/ подтвер- ждающая))
1						
2						

9. заявляет, что любые действия, которые будут совершены уполномоченными лицами Клиента с использованием ключа ЭП/КЭП ФНС/Простой ЭП, являются действиями, совершаемыми от имени Клиента, по его указанию и связаны с участием Клиента в электронном документообороте. Настоящее Заявление составлено в двух экземплярах, имеющих одинаковую юридическую силу. Один экземпляр хранится в Банке, второй – у Клиента.

В соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»

Я, _____
(ФИО) _____
(должность, наименование организации)

- ☐ - даю согласие на обработку моих персональных данных в целях исполнения настоящего договора
☐ - выступаю Оператором и даю поручение на осуществление другим лицом обработки персональных данных лиц, чьи персональные данные мною предоставлены в рамках исполнения настоящего договора

Клиент:

(подпись) / _____ Ф. И. О. / «__» _____ 20__ г.

М.П.

ОТМЕТКИ БАНКА:

Дата приема Заявления «__» _____ 20__ г.

Подключить к Системе «Интернет-банк». На условиях, определенных «Правилами подключения и эксплуатации дистанционного банковского обслуживания в Системе «Интернет-банк» в АО «БАНК ОРЕНБУРГ», заключен договор дистанционного банковского обслуживания № _____

АКЦЕПТ:

Уполномоченный работник, действующий на основании _____

(должность) / _____ (подпись) / _____ Ф. И. О.

БАНК:

АО «БАНК ОРЕНБУРГ», ИНН/КПП 5612031491/561201001

БИК 045354885, к/с 30101810400000000885 в Отделении Оренбург

РОССИЯ, 460024, Оренбургская обл., г. Оренбург, ул. Маршала Г. К. Жукова, зд. 25.

М. П.

Уполномоченный работник Банка, принявший Заявление

(подпись) / _____ Ф. И. О. / «__» _____ 20__ г.

⁵ Если доступ предоставляется уполномоченному лицу ЭП/КЭП ФНС/Простой ЭП которым предоставлялся ранее.

⁶ Указанные уполномоченные лица должны быть включены в карточку с образцами подписей и оттиска печати Клиента, за исключением лиц, которым в соответствии с п. 6.3.7. настоящих Правил предоставлена подтверждающая подпись.

Приложение № 4

**к Правилам подключения и эксплуатации дистанционного банковского обслуживания
в Системе «Интернет-банк»**

Агенту Удостоверяющего центра «AUTHORITY»,
АО «БАНК ОРЕНБУРГ»,
в Удостоверяющий центр «AUTHORITY»

**ЗАЯВЛЕНИЕ НА ВЫДАЧУ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ
ПОДПИСИ**

Прошу Удостоверяющий центр «AUTHORITY» создать и выдать уполномоченному лицу организации _____ (наименование организации) действующему(-ей) на основании _____, Сертификат ключа проверки электронной подписи (Класс 2 Сертификата).

С Правилами Электронного документооборота корпоративной информационной Системы «BeSafe» (далее – «Система «BeSafe»»), которые расположены в сети «Интернет» по адресу www.besafe.ru ознакомлен, согласен и обязуюсь выполнять.

Признаю, что получение документа, подписанного Электронной подписью Участника Системы «BeSafe» (далее – «Участник»), юридически эквивалентно получению документа на бумажном носителе, заверенного собственноручными подписями уполномоченных лиц Участника и оттиском печати Участника, если документ на бумажном носителе должен быть заверен печатью. Обязательства, предусмотренные настоящим пунктом, действительны при условии, что Ключ электронной подписи, Электронная подпись и Сертификат ключа проверки электронной подписи Участника созданы в соответствии с Правилами работы Удостоверяющего центра «AUTHORITY».

Реквизиты Клиента:

ФИО уполномоченного лица организации	
Наименование организации	
Контактный номер телефона	
E-mail	

Настоящим соглашаюсь с обработкой своих персональных данных, в том числе с использованием технических средств, Закрытым акционерным обществом «Центр Цифровых сертификатов», а также Агентом (Доверенным лицом) Удостоверяющего центра «AUTHORITY».

Признаю, что мои персональные данные, включенные в Сертификат, будут внесены Удостоверяющим центром в реестр Сертификатов. Реестр Сертификатов доступен в сети Интернет на сайте www.authority.ru.

Понимаю, что Удостоверяющий центр обрабатывает мои персональные данные, включенные в Сертификат и размещенные в реестре Сертификатов, для выполнения обязанностей по ведению реестра Сертификатов, включению содержащихся в Сертификатах персональных данных в реестр Сертификатов и обеспечению доступа лиц к информации, содержащейся в реестре Сертификатов с использованием сети Интернет, которые возложены на Удостоверяющий центр частью 2 статьи 13 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Понимаю, что в соответствии с пунктом 2 части 1 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» выполнение Удостоверяющим центром обязанностей, возложенных на него частью 2 статьи 13 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», является правовым основанием обработки моих персональных данных, включенных в Сертификат.

_____ (подпись уполномоченного лица организации)

_____ (Ф.И.О. уполномоченного лица организации)

М.П.

принято Агентом Удостоверяющего центра / Удостоверяющим центром:

_____ (наименование)

_____ (дата)

_____ (подпись уполномоченного лица)

_____ (Ф. И. О. уполномоченного лица)

М. П.

Приложение № 5
к Правилам подключения и эксплуатации дистанционного банковского обслуживания
в Системе «Интернет-банк»

Заявление на выдачу Простой ЭП

Полное наименование Клиента	
ИНН/ОГРН/ОГРНИП	
в лице (должность Ф. И. О. полностью)	
действующего на основании	☐ Устава ☐ Свидетельства ☐ Доверенности №__ от «__» _____ 20__ г.
Юридический адрес	
Телефон, e-mail	

В соответствии с Правилами подключения и эксплуатации систем дистанционного банковского обслуживания в Системе «Интернет-банк» в АО «БАНК ОРЕНБУРГ», прошу выдать Логин и Пароль⁷ уполномоченному лицу организации:

№	Уполномоченные лица (должность Ф. И. О. полностью) ⁸	Телефон для получения разовых паролей
1		
2		

с Правилами Электронного документооборота корпоративной информационной Системы «BeSafe» (далее – Система «BeSafe»), которые расположены в сети «Интернет» по адресу www.besafe.ru ознакомлен, согласен и обязуюсь выполнять.

Признаю, что получение документа, подписанного Простой ЭП Участника, юридически эквивалентно получению документа на бумажном носителе, заверенного собственноручной подписью Участника. Обязательства, предусмотренные настоящим пунктом, действительны при условии, что Простая ЭП Участника создана с использованием технологии Системы «BeSafe».

Заявляю, что любые действия, которые будут совершены уполномоченным лицом с использованием Простой ЭП, полученной на основании настоящего Заявления, являются действиями, совершаемыми от имени Клиента, по его указанию и связаны с участием Клиента в электронном документообороте.

Клиент:

_____/_____/«__» _____ 20__ г.
(подпись) Ф. И. О.

М. П.

Банк:

Уполномоченный работник Банка, принявший Заявление

_____/_____/«__» _____ 20__ г.
(подпись) Ф. И. О.

М. П.

⁷ Логин отправляется на электронную почту, указанную в заявлении, пароль отправляется на номер телефона для получения разовых паролей.

⁸ Указанные уполномоченные лица должны быть включены в карточку с образцами подписей и отиска печати Клиента, за исключением лиц, которым в соответствии с п. 6.3.7. настоящих Правил предоставлена подтверждающая подпись.

Приложение № 6

**к Правилам подключения и эксплуатации дистанционного банковского обслуживания
в Системе «Интернет-банк»**

Агенту Удостоверяющего центра "AUTHORITY"
АО "БАНК ОРЕНБУРГ",
в Удостоверяющий центр "AUTHORITY"

**ЗАЯВЛЕНИЕ НА ВЫДАЧУ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ
ПОДПИСИ**

Прошу Удостоверяющий центр "AUTHORITY" создать и выдать мне, Сертификат ключа проверки электронной подписи (Класс 2 Сертификата) для физического лица.

С Правилами Электронного документооборота корпоративной информационной Системы "BeSafe" (далее - "Система "BeSafe"), которые расположены в сети "Интернет" по адресу www.besafe.ru ознакомлен, согласен и обязуюсь выполнять.

Признаю, что получение документа, подписанного Электронной подписью Участника Системы "BeSafe" (далее - "Участник"), юридически эквивалентно получению документа на бумажном носителе, заверенного собственноручными подписями уполномоченных лиц Участника и оттиском печати Участника. Обязательства, предусмотренные настоящим пунктом, действительны при условии, что Ключ электронной подписи, Электронная подпись и Сертификат ключа проверки электронной подписи Участника созданы в соответствии с Правилами работы Удостоверяющего центра "AUTHORITY".

Реквизиты *Клиента*:

Ф. И. О.	
Контактный номер телефона	
E-mail	

Настоящим соглашаюсь с обработкой своих персональных данных, в том числе с использованием технических средств, Закрытым акционерным обществом "Центр Цифровых сертификатов", а также Агентом (Доверенным лицом) Удостоверяющего центра "AUTHORITY".

Признаю, что мои персональные данные, включенные в Сертификат, будут внесены Удостоверяющим центром в реестр Сертификатов. Реестр Сертификатов доступен в сети Интернет на сайте www.authority.ru.

Понимаю, что Удостоверяющий центр обрабатывает мои персональные данные, включенные в Сертификат и размещенные в реестре Сертификатов, для выполнения обязанностей по ведению реестра Сертификатов, включению содержащихся в Сертификатах персональных данных в реестр Сертификатов и обеспечению доступа лиц к информации, содержащейся в реестре Сертификатов с использованием сети Интернет, которые возложены на Удостоверяющий центр частью 2 статьи 13 Федерального закона от 6 апреля 2011 года № 63-ФЗ "Об электронной подписи".

Понимаю, что в соответствии с пунктом 2 части 1 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" выполнение Удостоверяющим центром обязанностей, возложенных на него частью 2 статьи 13 Федерального закона от 6 апреля 2011 года № 63-ФЗ "Об электронной подписи", является правовым основанием обработки моих персональных данных, включенных в Сертификат.

_____ (подпись Клиента)

_____ (Ф. И. О. Клиента)

принято Агентом Удостоверяющего центра / Удостоверяющим центром:

_____ (наименование)

_____ (дата)

_____ (подпись уполномоченного лица)

_____ (Ф. И. О. уполномоченного лица)

М. П.

Приложение № 7

**к Правилам подключения и эксплуатации дистанционного банковского обслуживания
в Системе «Интернет-банк»**

Заявление на внесение изменений в Систему «Интернет-банк»

Настоящим заявлением Клиент:

Полное наименование Клиента	
ИНН/ОГРН/ОГРНИП	
в лице (должность Ф. И. О. полностью)	
действующего на основании	☐ Устава ☐ Свидетельства ☐ Доверенности № ____ от « ____ » _____ 20 ____ г.
Юридический адрес	
Телефон, e-mail	

в связи:

- | | |
|---|--|
| ☐ со сменой уполномоченного лица; | ☐ с утерей смарт-ключа; |
| ☐ со сменой Ф. И. О. уполномоченного лица; | ☐ с компрометацией; |
| ☐ с истечением срока действия сертификата; | ☐ с технической неисправностью смарт-ключа; |
| ☐ со сменой наименования; | ☐ со сменой адреса; |
| ☐ прочее _____ | |

прошу внести следующие изменения в Системе «Интернет-банк» с « ____ » _____ 20 ____ г., и предоставить доступ к Системе «Интернет-банк» уполномоченным лицам с правами для выполнения операций с использованием счетов, указанных в настоящем Заявлении:

№	Номер счета	Уполномоченные лица (должность Ф.И.О. полностью) ⁹	Разрешено запрашивать выписку (да/нет)	Разрешено создавать платежные документы (да/нет)	Разрешено подписывать и отправлять документы (да/нет)	Тип подписи (первая/ вторая/ подтвер- ждающая)
1						
2						

Заявляю, что любые действия, которые будут совершены уполномоченными лицами на основании настоящего Заявления, являются действиями, совершаемыми от имени Клиента, по его указанию и связаны с участием Клиента в электронном документообороте.

Клиент:

_____/_____/« ____ » _____ 20 ____ г.
(подпись) Ф. И. О. М.П.

Банк:

Уполномоченный работник Банка, принявший Заявление

_____/_____/« ____ » _____ 20 ____ г.
(подпись) Ф. И. О.

⁹ Указанные уполномоченные лица должны быть включены в карточку с образцами подписей и оттиска печати Клиента, за исключением лиц, которым в соответствии с п. 6.3.7. настоящих Правил предоставлена подтверждающая подпись.

**УВЕДОМЛЕНИЕ О КОМПРОМЕТАЦИИ СЕКРЕТНОГО КЛЮЧА,
СРЕДСТВ ПРОСТОЙ ЭП**

Полное наименование Клиента	
ИНН/ОГРН/ОГРНИП	
в лице (должность Ф.И.О. полностью)	
действующего на основании	☐ Устава ☐ Свидетельства ☐ Доверенности №__ от «__» _____ 20__ г.
Юридический адрес	
Телефон, e-mail	

Сообщаем о факте компрометации СЕКРЕТНОГО КЛЮЧА, ПАРОЛЯ которому соответствует указанный ниже сертификат.

Прошу блокировать данный СЕРТИФИКАТ в Системе «Интернет-банк»:

Ф.И.О. Владельца сертификата	
Идентификатор владельца сертификата	
Контакты владельца сертификата (телефон, e-mail)	

Клиент:

_____/_____/«__»____20__ г.
(подпись) Ф. И. О. М. П.

Банк:

Уполномоченный работник Банка, принявший Заявление

_____/_____/«__»____20__ г.
(подпись) Ф. И. О.

время

**Правила обмена электронными сообщениями
по Системе «Интернет-банк»»**

1.1. Стороны имеют право обмениваться электронными сообщениями. Вложенные в сообщения Клиента файлы (документы), отправленные в Банк по Системе «Интернет-банк» (если возможность направления вложенных файлов (документов) по Системе «Интернет-банк» для целей соответствующего соглашения Сторон не исключена (или не ограничена) условиями такого соглашения), признаются подписанными уполномоченными лицами Клиента и приравниваются к документам, составленным на бумажном носителе, если сообщение, в которое был вложен файл, составлено и заверено корректной ЭП/КЭП ФНС/Простой ЭП Клиента. При этом на вложении визуальное ЭП/КЭП ФНС/ Простая ЭП Клиента отсутствует, подтверждением является полученное сообщение.

1.2. В случае если сообщение с вложенным файлом используется в целях предоставления Банку Клиентом изображения документа, полученного с использованием сканирующих устройств, (в том числе в соответствии с условиями заключенных между Банком и Клиентом соглашений), то изображение документа, полученного с использованием сканирующих устройств, вложенного в сообщение, направляемое по Системе «Интернет-банк», считается заверенным Клиентом, если такое сообщение составлено и заверено корректной ЭП/КЭП ФНС/Простой ЭП Клиента, при этом на вложении визуальное ЭП/КЭП ФНС/Простая ЭП Клиента отсутствует, подтверждением является полученное сообщение.

1.3. Стороны признают, что подделка ЭП/КЭП ФНС/Простой ЭП сторон, то есть создание корректной ЭП/Простой ЭП в сообщении от имени Сторон, невозможна без знания закрытых ключей электронной подписи, средств Простой ЭП Сторон. Стороны согласны, что подтверждение корректности ЭП/КЭП ФНС/Простой ЭП при передаче сообщения позволяет достоверно установить, что сообщение и вложенные файлы исходят от стороны по Договору, чья ЭП/КЭП ФНС/ Простая ЭП которая содержится в сообщении и является подлинной.

1.4. Стороны признают в качестве единой шкалы времени при работе с Системой местное время. Контрольным является время системных часов аппаратных средств Банка.